(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号
特開2000－331420
（P2000－331420A）
(43)公開日　平成12年11月30日(2000.11.30)

(51)Int.Cl.[7]	識別記号	FI	テーマコード（参考）
G11B 20/10		G11B 20/10	H
G06F 3/06	304	G06F 3/06	304M
12/14	320	12/14	320B
G09C 1/00	660	G09C 1/00	660D
G10L 11/00		G10L 9/00	E

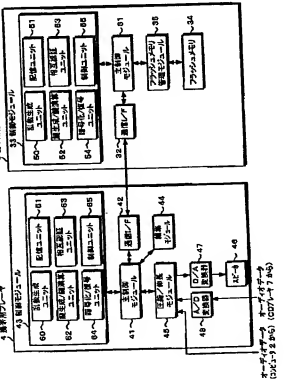
審査請求　未請求　請求項の数43　ＯＬ　（全 38 頁）　最終頁に続く

(21)出願番号　特願2000－76390(P2000－76390)
(22)出願日　平成12年３月14日(2000.3.14)
(31)優先権主張番号　特願平11－69153
(32)優先日　平成11年３月15日(1999.3.15)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　大石　丈於
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　岡上　拓己
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082762
弁理士　杉浦　正知

(54)【発明の名称】　データ処理装置、記憶装置、データ処理システムおよびその方法

(57)【要約】
【課題】　編集処理などが行われ、既に暗号化されたトラックデータに異なる鍵データが割り当てられた場合の処理の時間を短縮する。
【解決手段】　携帯用プレーヤ４のＳＡＭ４３において、コンテンツ鍵データＣＫとパーツ鍵データＰＫとのＸＯＲを演算してテンポラリ鍵データＴＭＫを生成し、テンポラリ鍵データＴＭＫとブロックシードデータＢＳとのＭＡＣ演算を行ってブロック毎にブロック鍵データＢＫを生成する。そして、オーディオデータをブロック毎にブロック鍵データＢＫを用いて暗号化してフラッシュメモリ３４に記憶する。コンテンツ鍵データＣＫが変更になった場合には、テンポラリ鍵データＴＭＫが変わらないように、パーツ鍵データＰＫを変更する。



【特許請求の範囲】

【請求項１】　単数または複数の関連するモジュールから構成されるトラックデータを、当該トラックデータに割り当てられた第１の鍵データおよび上記モジュール毎に割り当てられた第２の鍵データを用いて暗号化して記憶装置に出力するデータ処理装置において、

上記モジュール毎に、上記第１の鍵データおよび上記モジュールに割り当てられた上記第２の鍵データから第３の鍵データを算出する鍵データ算出手段と、

上記トラックデータを上記モジュール毎に当該モジュールの上記第３の鍵データに応じて暗号化して上記記憶装置に出力する暗号化手段とを有し、

上記データ算出手段は、上記第１の鍵データに変更があった場合に、上記第３の鍵データを変更しないように、上記モジュール毎に上記第２の鍵データを変更するデータ処理装置。

【請求項２】　請求項１において、

上記鍵データ算出手段は、編集によって上記モジュールが、上記トラックデータに割り当てられた上記第１の鍵データとは異なる上記第１の鍵データが割り当てられた新たなトラックデータに属するようになったときに、上記モジュール毎に、上記第３の鍵データを変更しないように、上記第２の鍵データを変更するデータ処理装置。

【請求項３】　請求項１において、

上記モジュールは、単数または複数のサブモジュールを有し、上記サブモジュール毎に第４の鍵データがさらに割り当てられている場合に、

上記サブモジュール毎に、上記第３の鍵データおよび上記サブモジュールに割り当てられた上記第４の鍵データから第５の鍵データを算出し、

上記暗号化手段は、上記トラックデータを上記サブモジュール毎に当該サブモジュールの上記第５の鍵データを用いて暗号化して上記記憶装置に出力するデータ処理装置。

【請求項４】　請求項３において、

上記鍵データ算出手段は、上記第３の鍵データおよび上記第４の鍵データを引数とする一方向性ハッシュ関数を用いて、上記第５の鍵データを算出するデータ処理装置。

【請求項５】　請求項４において、

上記一方向性ハッシュ関数は、ＭＡＣ演算を行う関数であるデータ処理装置。

【請求項６】　請求項１において、

上記鍵データ算出手段は、論理演算を行って上記第３の鍵データを算出するデータ処理装置。

【請求項７】　請求項１において、

上記データ処理装置は、

上記変更した第２の鍵データを上記記憶装置に書き込むデータ処理装置。

【請求項８】　請求項１において、

上記鍵データ算出手段は、

上記第１の鍵データおよび上記第２の鍵データを、それぞれ乱数を発生して生成するデータ処理装置。

【請求項９】　請求項８において、

上記データ処理装置は、

上記記憶装置によって暗号化された上記第１の鍵データと上記第２の鍵データとを上記記憶装置に書き込むデータ処理装置。

【請求項１０】　請求項３において、

上記鍵データ算出手段は、、

上記第４の鍵データを、乱数を発生して生成するデータ処理装置。

【請求項１１】　請求項１０において、

上記データ処理装置は、

上記生成した第４の鍵データを上記記憶装置に書き込むデータ処理装置。

【請求項１２】　請求項１において、

上記記憶装置との間で相互認証を行う相互認証手段をさらに有し、

上記暗号化手段は、上記相互認証によって上記記憶装置の正当性が認められたときにのみ、上記第１の鍵データを生成するデータ処理装置。

【請求項１３】　記憶装置から入力した単数または複数の関連するモジュールから構成されるトラックデータを、当該トラックデータに割り当てられた第１の鍵データおよび上記モジュール毎に割り当てられた第２の鍵データを用いて復号するデータ処理装置において、

上記モジュール毎に、上記第１の鍵データおよび上記モジュールに割り当てられた上記第２の鍵データから第３の鍵データを算出する鍵データ算出手段と、

上記記憶装置から入力した上記トラックデータを上記モジュール毎に当該モジュールの上記第３の鍵データに応じて復号する復号手段とを有し、

上記鍵データ算出手段は、上記第１の鍵データに変更があった場合に、上記第３の鍵データを変更しないように、上記モジュール毎に上記第２の鍵データを変更するデータ処理装置。

【請求項１４】　請求項１３において、

上記鍵データ算出手段は、編集によって上記モジュールが、上記トラックデータとは異なる上記第１の鍵データが割り当てられた新たなトラックデータに属するようになったときに、上記モジュール毎に、上記第３の鍵データを変更しないように上記第２の鍵データを変更するデータ処理装置。

【請求項１５】　請求項１３において、

上記モジュールは、単数または複数のサブモジュールを有し、上記サブモジュール毎に第４の鍵データがさらに割り当てられている場合に、

上記鍵データ算出手段は、上記サブモジュール毎に、上記第３の鍵データおよび上記サブモジュールに割り当て

られた上記第４の鍵データから第５の鍵データを算出し、
上記復号手段は、上記記憶装置から入力した上記トラックデータを上記サブモジュール毎に当該サブモジュールの上記第５の鍵データを用いて復号するデータ処理装置。
【請求項１６】　請求項１５において、
上記鍵データ算出手段は、上記第３の鍵データおよび上記第４の鍵データを引数とする一方向性ハッシュ関数を用いて、上記第５の鍵データを算出するデータ処理装置。
【請求項１７】　請求項１６において、
上記一方向性ハッシュ関数は、ＭＡＣ演算を行う関数であるデータ処理装置。
【請求項１８】　請求項１３において、
上記鍵データ算出手段は、論理演算を行って上記第３の鍵データを算出するデータ処理装置。
【請求項１９】　請求項１３において、
上記データ処理装置は、上記変更した第２の鍵データを上記記憶装置に書き込むデータ処理装置。
【請求項２０】　請求項１３において、
上記データ処理装置は、上記第１の鍵データおよび上記第２の鍵データを上記記憶装置から読み出すデータ処理装置。
【請求項２１】　請求項１５において、
上記データ処理装置は、上記第４の鍵データを上記記憶装置から読み出すデータ処理装置。
【請求項２２】　請求項１３において、
上記記憶装置との間で相互認証を行う相互認証手段をさらに有し、
上記復号手段は、上記相互認証によって上記記憶装置の正当性が認められたときにのみ、上記記憶装置から上記第１の鍵データを入力検出するデータ処理装置。
【請求項２３】　記憶装置とデータ処理装置との間で、単数または複数の関連するモジュールから構成されるトラックデータを入出力するデータ処理システムにおいて、
上記記憶装置は、記憶手段を有し、
上記データ処理装置は、上記モジュール毎に、上記トラックデータに割り当てられた第１の鍵データおよび上記モジュール毎に割り当てられた第２の鍵データから第３の鍵データを算出する鍵データ算出手段と、
上記トラックデータを上記モジュール毎に当該モジュールの上記第３の鍵データに応じて暗号化して上記記憶装置に出力する暗号化手段とを有し、
上記鍵データ算出手段は、上記第１の鍵データに変更があった場合に、上記第３の鍵データを変更しないように、上記モジュール毎に上記第２の鍵データを変更するデータ処理システム。
【請求項２４】　請求項２３において、
上記鍵データ算出手段は、編集によって上記モジュールが、上記トラックデータに割り当てられた上記第１の鍵データとは異なる上記第１の鍵データが割り当てられた新たなトラックデータに属するようになったときに、上記モジュール毎に、上記第３の鍵データを変更しないように上記第２の鍵データを変更するデータ処理システム。
【請求項２５】　請求項２３において、
上記モジュールは、単数または複数のサブモジュールを有し、上記サブモジュール毎に第４の鍵データがさらに割り当てられている場合に、
上記データ処理装置は、上記鍵データ算出手段によって、上記サブモジュール毎に、上記第３の鍵データおよび上記サブモジュールに割り当てられた上記第４の鍵データから第５の鍵データを算出し、
上記暗号化手段は、上記トラックデータを上記サブモジュール毎に当該サブモジュールの上記第５の鍵データを用いて暗号化して上記記憶装置に出力するデータ処理システム。
【請求項２６】　請求項２５において、
上記鍵データ算出手段は、上記第３の鍵データおよび上記第４の鍵データを引数とする一方向性ハッシュ関数を用いて、上記第５の鍵データを算出するデータ処理システム。
【請求項２７】　請求項２３において、
上記記憶装置は、第１の相互認証処理手段をさらに有し、
上記データ処理装置は、上記第１の相互認証処理手段との間で相互認証を行う第２の相互認証処理手段をさらに有するデータ処理システム。
【請求項２８】　記憶装置とデータ処理装置との間で、単数または複数の関連するモジュールから構成されるトラックデータを入出力するデータ処理システムにおいて、
上記記憶装置は、記憶手段を有し、
上記データ処理装置は、上記モジュール毎に、上記トラックデータに割り当てられた第１の鍵データおよび上記モジュール毎に割り当てられた上記第２の鍵データから第３の鍵データを算出する鍵データ算出手段と、
上記記憶装置から入力した上記トラックデータを上記モジュール毎に当該モジュールの上記第３の鍵データに応じて復号する復号手段とを有し、
上記鍵データ算出手段は、上記第１の鍵データに変更があった場合に、上記第３の鍵データを変更しないように、上記モジュール毎に上記第２の鍵データを変更するデータ処理システム。
【請求項２９】　請求項２８において、
上記鍵データ算出手段は、編集によって上記モジュールが、上記トラックデータとは異なる上記第１の鍵データが割り当てられた新たなトラックデータに属するように

なったときに、上記モジュール毎に、上記第３の鍵データを変更しないように上記第２の鍵データを変更するデータ処理システム。

【請求項３０】　請求項２８において、

上記モジュールは、単数または複数のサブモジュールを有し、上記サブモジュール毎に第４の鍵データがさらに割り当てられている場合に、

上記データ処理装置は、上記鍵データ算出手段によって、上記サブモジュール毎に、上記第３の鍵データおよび上記サブモジュールに割り当てられた上記第４の鍵データから第５の鍵データを算出し、

上記復号手段は、上記記憶装置から入力した上記トラックデータを上記サブモジュール毎に当該サブモジュールの上記第５の鍵データを用いて復号するデータ処理システム。

【請求項３１】　請求項２８において、

上記記憶装置は、第１の相互認証処理手段をさらに有し、

上記データ処理装置は、上記第１の相互認証処理手段との間で相互認証を行う第２の相互認証処理手段をさらに有するデータ処理システム。

【請求項３２】　単数または複数の関連するモジュールから構成されるトラックデータを、上記トラックデータに割り当てられた第１の鍵データおよび上記モジュール毎に割り当てられた第２の鍵データを用いて暗号化して記憶装置に記憶するデータ処理方法において、

上記モジュール毎に、上記第１の鍵データおよび上記モジュールに割り当てられた上記第２の鍵データから第３の鍵データを算出し、

上記トラックデータを上記モジュール毎に当該モジュールの上記第３の鍵データに応じて暗号化して上記記憶装置に出力し、

上記第１の鍵データに変更があった場合に、上記第３の鍵データを変更しないように、上記モジュール毎に上記第２の鍵データを変更するデータ処理方法。

【請求項３３】　請求項３２において、

編集によって上記モジュールが、上記トラックデータに割り当てられた上記第１の鍵データとは異なる上記第１の鍵データが割り当てられた新たなトラックデータに属するようになったときに、上記モジュール毎に、上記第３の鍵データを変更しないように、上記第２の鍵データを変更するデータ処理方法。

【請求項３４】　請求項３２において、

上記モジュールは、単数または複数のサブモジュールを有し、上記サブモジュール毎に第４の鍵データがさらに割り当てられている場合に、

上記サブモジュール毎に、上記第３の鍵データおよび上記サブモジュールに割り当てられた上記第４の鍵データから第５の鍵データを算出し、

上記トラックデータを上記サブモジュール毎に当該サブモジュールの上記第５の鍵データを用いて暗号化して上記記憶装置に出力するデータ処理方法。

【請求項３５】　請求項３４において、

上記第３の鍵データおよび上記第４の鍵データを引数とする一方向性ハッシュ関数を用いて、上記第５の鍵データを算出するデータ処理方法。

【請求項３６】　記憶装置から入力した単数または複数の関連するモジュールから構成されるトラックデータを、上記トラックデータに割り当てられた第１の鍵データおよび上記モジュール毎に割り当てられた第２の鍵データを用いて復号するデータ処理方法において、

上記モジュール毎に、上記第１の鍵データおよび上記モジュールに割り当てられた上記第２の鍵データから第３の鍵データを算出し、

上記記憶装置から入力した上記トラックデータを上記モジュール毎に当該モジュールの上記第３の鍵データに応じて復号し、

上記第１の鍵データに変更があった場合に、上記第３の鍵データを変更しないように、上記モジュール毎に上記第２の鍵データを変更するデータ処理方法。

【請求項３７】　請求項３６において、

編集によって上記モジュールが、上記トラックデータとは異なる上記第１の鍵データが割り当てられた新たなトラックデータに属するようになったときに、上記モジュール毎に、上記第３の鍵データを変更しないように上記第２の鍵データを変更するデータ処理方法。

【請求項３８】　請求項３６において、

上記モジュールは、単数または複数のサブモジュールを有し、上記サブモジュール毎に第４の鍵データがさらに割り当てられている場合に、

上記サブモジュール毎に、上記第３の鍵データおよび上記サブモジュールに割り当てられた上記第４の鍵データから第５の鍵データを算出し、

上記記憶装置から入力した上記トラックデータを上記サブモジュール毎に当該サブモジュールの上記第５の鍵データを用いて復号するデータ処理方法。

【請求項３９】　請求項３８において、

上記第３の鍵データおよび上記第４の鍵データを引数とする一方向性ハッシュ関数を用いて、上記第５の鍵データを算出するデータ処理方法。

【請求項４０】　ディジタルデータを暗号化するデータ処理装置において、

コンテンツ鍵をセッション鍵で暗号化する暗号化手段と、

上記セッション鍵で暗号化されたコンテンツ鍵を記憶装置に出力するとともに、上記記憶装置の記憶用鍵データで暗号化されたコンテンツ鍵を上記記憶装置から入力するインターフェイス手段とを備え、

上記暗号化手段は、上記ディジタルデータを上記記憶用鍵データで暗号化されたコンテンツ鍵に基づいて暗号化

し、
上記インターフェイス手段は、上記暗号化されたディジタルデータを上記記憶用鍵データで暗号化されたコンテンツ鍵とともに上記記憶装置に出力するデータ処理装置。

【請求項４１】　暗号化されたディジタルデータを記憶する記憶装置において、
コンテンツ鍵をセッション鍵で復号する復号手段と、
復号されたコンテンツ鍵を記憶用鍵データで暗号化する暗号化手段と、
セッション鍵で暗号化されたコンテンツ鍵をデータ処理装置から入力し、上記記憶用鍵データで暗号化されたコンテンツ鍵を上記データ処理装置に出力し、上記暗号化されたディジタルデータを上記記憶用鍵データで暗号化されたコンテンツ鍵とともに上記データ処理装置から入力するインターフェイス手段と、
上記データ処理装置から入力された暗号化されたディジタルデータとコンテンツ鍵を記憶するメモリ手段とを備える記憶装置。

【請求項４２】　データ処理装置と記憶装置との間でディジタルデータを入出力するデータ処理システムにおいて、
上記データ処理装置は、
コンテンツ鍵をセッション鍵で暗号化する第１の暗号化手段と、
上記セッション鍵で暗号化されたコンテンツ鍵を上記記憶装置に出力するとともに、上記記憶装置の記憶用鍵データで暗号化されたコンテンツ鍵を上記記憶装置から入力する第１のインターフェイス手段とを備え、
上記第１の暗号化手段は、上記ディジタルデータを上記記憶用鍵データで暗号化されたコンテンツ鍵に基づいて暗号化し、
上記第１のインターフェイス手段は、上記暗号化されたディジタルデータを上記記憶用鍵データで暗号化されたコンテンツ鍵とともに上記記憶装置に出力し、
上記記憶装置は、
上記データ処理装置からのコンテンツ鍵をセッション鍵で復号する復号手段と、
復号されたコンテンツ鍵を記憶用鍵データで暗号化する第２の暗号化手段と、
セッション鍵で暗号化されたコンテンツ鍵を上記データ処理装置から入力し、上記記憶用鍵データで暗号化されたコンテンツ鍵を上記データ処理装置に出力し、上記暗号化されたディジタルデータを上記記憶用鍵データで暗号化されたコンテンツ鍵とともに上記データ処理装置から入力する第２のインターフェイス手段と、
上記データ処理装置から入力された暗号化されたディジタルデータとコンテンツ鍵を記憶するメモリ手段とを備えるデータ処理システム。

【請求項４３】　データ処理装置と記憶装置との間でディジタルデータを入出力するデータ処理方法において、
コンテンツ鍵をセッション鍵で暗号化するステップと、
上記セッション鍵で暗号化されたコンテンツ鍵を上記データ処理装置から上記記憶装置に送出するステップと、
上記データ処理装置からのコンテンツ鍵をセッション鍵で復号するステップと、
復号されたコンテンツ鍵を上記記憶装置の記憶用鍵データで暗号化するステップと、
記憶用鍵データで暗号化されたコンテンツ鍵を上記記憶装置から上記データ処理装置に送出するステップと、
上記ディジタルデータを上記記憶装置からのコンテンツ鍵に基づいて暗号化するステップと、
上記暗号化されたディジタルデータを上記記憶用鍵データで暗号化されたコンテンツ鍵とともに上記データ処理装置から上記記憶装置に送出するステップと、
上記データ処理装置からの暗号化されたディジタルデータとコンテンツ鍵を記憶するステップとを備えるデータ処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、楽曲などの単数または複数の関連するモジュールから構成されるトラックデータを暗号化して記憶装置に記憶するデータ処理装置、記憶装置、データ処理システムおよびその方法に関する。

【０００２】

【従来の技術】例えば、著作権侵害となる不正利用を防止するために、１曲分のオーディオデータなどの複数の関連するモジュールから構成されるトラックデータを暗号化して記憶媒体に記憶することがある。この場合に、解読を困難にするために、例えば、個々のトラックデータに割り当てられたコンテンツ鍵データと、当該トラック内に規定されたモジュール（パーツ）に割り当てられたパーツ鍵データとを用いて演算を行ってパーツ毎にブロック鍵データを生成し、パーツ毎に異なるブロック鍵データを用いてトラックデータを暗号化する。

【０００３】

【発明が解決しようとする課題】ところで、上述したブロック鍵データを用いてトラックデータを暗号化した場合に、例えば、編集処理などが行われて、既に暗号化されたパーツが以前とは異なるコンテンツ鍵データが割り当てられた新たなトラックデータに属するようになった場合に、当該コンテンツ鍵データの変更に応じて、当該パーツに用いられるブロック鍵データが変わってしまう。その結果、当該パーツを復号した後に、再度、新たなブロック鍵データを用いて暗号化する必要が生じる。しかしながら、編集処理を行う度に、既に暗号化したトラックデータの復号および再暗号化を行うのでは、編集処理の負荷が重くなり、編集時間が長くなるという問題がある。

【０００４】この発明の目的は、上述した従来技術の問題点に鑑みてなされ、編集処理などが行われ、既に暗号化されたトラックデータに異なる鍵データが割り当てられた場合の処理の時間を短縮できるデータ処理装置、記憶装置、データ処理システムおよびその方法を提供することにある。

【０００５】

【課題を解決するための手段】上述した課題を解決するために、請求項１の発明は、単数または複数の関連するモジュールから構成されるトラックデータを、当該トラックデータに割り当てられた第１の鍵データおよびモジュール毎に割り当てられた第２の鍵データを用いて暗号化して記憶装置に出力するデータ処理装置において、モジュール毎に、第１の鍵データおよびモジュールに割り当てられた第２の鍵データから第３の鍵データを算出する鍵データ算出手段と、トラックデータをモジュール毎に当該モジュールの第３の鍵データに応じて暗号化して記憶装置に出力する暗号化手段とを有し、データ算出手段は、第１の鍵データに変更があった場合に、第３の鍵データを変更しないように、モジュール毎に第２の鍵データを変更するデータ処理装置である。

【０００６】請求項１のデータ処理装置では、第１の鍵データが変更された場合でも、鍵データ処理手段によって第３の鍵データを変更しないように第２の鍵データが変更されるため、記憶装置に記憶した暗号化されたトラックデータを復号して再度暗号化する必要がなくなる。

【０００７】請求項１３の発明は、記憶装置から入力した単数または複数の関連するモジュールから構成されるトラックデータを、当該トラックデータに割り当てられた第１の鍵データおよびモジュール毎に割り当てられた第２の鍵データを用いて復号するデータ処理装置において、モジュール毎に、第１の鍵データおよびモジュールに割り当てられた第２の鍵データから第３の鍵データを算出する鍵データ算出手段と、記憶装置から入力したトラックデータをモジュール毎に当該モジュールの第３の鍵データに応じて復号する復号手段とを有し、鍵データ算出手段は、第１の鍵データに変更があった場合に、第３の鍵データを変更しないように、モジュール毎に第２の鍵データを変更するデータ処理装置である。

【０００８】請求項２３の発明は、記憶装置とデータ処理装置との間で、単数または複数の関連するモジュールから構成されるトラックデータを入出力するデータ処理システムにおいて、記憶装置は、記憶手段を有し、データ処理装置は、モジュール毎に、トラックデータに割り当てられた第１の鍵データおよびモジュール毎に割り当てられた第２の鍵データから第３の鍵データを算出する鍵データ算出手段と、トラックデータをモジュール毎に当該モジュールの第３の鍵データに応じて暗号化して記憶装置に出力する暗号化手段とを有し、鍵データ算出手段は、第１の鍵データに変更があった場合に、第３の鍵データを変更しないように、モジュール毎に第２の鍵データを変更するデータ処理システムである。

【０００９】請求項２８の発明は、記憶装置とデータ処理装置との間で、単数または複数の関連するモジュールから構成されるトラックデータを入出力するデータ処理システムにおいて、記憶装置は、記憶手段を有し、データ処理装置は、モジュール毎に、トラックデータに割り当てられた第１の鍵データおよびモジュール毎に割り当てられた第２の鍵データから第３の鍵データを算出する鍵データ算出手段と、記憶装置から入力したトラックデータをモジュール毎に当該モジュールの第３の鍵データに応じて復号する復号手段とを有し、鍵データ算出手段は、第１の鍵データに変更があった場合に、第３の鍵データを変更しないように、モジュール毎に第２の鍵データを変更するデータ処理システムである。

【００１０】請求項３２の発明は、単数または複数の関連するモジュールから構成されるトラックデータを、トラックデータに割り当てられた第１の鍵データおよびモジュール毎に割り当てられた第２の鍵データを用いて暗号化して記憶装置に記憶するデータ処理方法において、モジュール毎に、第１の鍵データおよびモジュールに割り当てられた第２の鍵データから第３の鍵データを算出し、トラックデータをモジュール毎に当該モジュールの第３の鍵データに応じて暗号化して記憶装置に出力し、第１の鍵データに変更があった場合に、第３の鍵データを変更しないように、モジュール毎に第２の鍵データを変更するデータ処理方法である。

【００１１】請求項３６の発明は、記憶装置から入力した単数または複数の関連するモジュールから構成されるトラックデータを、トラックデータに割り当てられた第１の鍵データおよびモジュール毎に割り当てられた第２の鍵データを用いて復号するデータ処理方法において、モジュール毎に、第１の鍵データおよびモジュールに割り当てられた第２の鍵データから第３の鍵データを算出し、記憶装置から入力したトラックデータをモジュール毎に当該モジュールの第３の鍵データに応じて復号し、第１の鍵データに変更があった場合に、第３の鍵データを変更しないように、モジュール毎に第２の鍵データを変更するデータ処理方法である。

【００１２】請求項４０の発明は、ディジタルデータを暗号化するデータ処理装置において、コンテンツ鍵をセッション鍵で暗号化する暗号化手段と、セッション鍵で暗号化されたコンテンツ鍵を記憶装置に出力するとともに、記憶装置の記憶用鍵データで暗号化されたコンテンツ鍵を記憶装置から入力するインターフェイス手段とを備え、暗号化手段は、ディジタルデータを記憶用鍵データで暗号化されたコンテンツ鍵に基づいて暗号化し、インターフェイス手段は、暗号化されたディジタルデータを記憶用鍵データで暗号化されたコンテンツ鍵とともに

記憶装置に出力するデータ処理装置である。

【００１３】請求項４１の発明は、暗号化されたディジタルデータを記憶する記憶装置において、コンテンツ鍵をセッション鍵で復号する復号手段と、復号されたコンテンツ鍵を記憶用鍵データで暗号化する暗号化手段と、セッション鍵で暗号化されたコンテンツ鍵をデータ処理装置から入力し、記憶用鍵データで暗号化されたコンテンツ鍵をデータ処理装置に出力し、暗号化されたディジタルデータを記憶用鍵データで暗号化されたコンテンツ鍵とともにデータ処理装置から入力するインターフェイス手段と、データ処理装置から入力された暗号化されたディジタルデータとコンテンツ鍵を記憶するメモリ手段とを備える記憶装置である。

【００１４】請求項４２の発明は、データ処理装置と記憶装置との間でディジタルデータを入出力するデータ処理システムにおいて、データ処理装置は、コンテンツ鍵をセッション鍵で暗号化する第１の暗号化手段と、セッション鍵で暗号化されたコンテンツ鍵を記憶装置に出力するとともに、記憶装置の記憶用鍵データで暗号化されたコンテンツ鍵を記憶装置から入力する第１のインターフェイス手段とを備え、第１の暗号化手段は、ディジタルデータを記憶用鍵データで暗号化されたコンテンツ鍵に基づいて暗号化し、第１のインターフェイス手段は、暗号化されたディジタルデータを記憶用鍵データで暗号化されたコンテンツ鍵とともに記憶装置に出力し、記憶装置は、データ処理装置からのコンテンツ鍵をセッション鍵で復号する復号手段と、復号されたコンテンツ鍵を記憶用鍵データで暗号化する第２の暗号化手段と、セッション鍵で暗号化されたコンテンツ鍵をデータ処理装置から入力し、記憶用鍵データで暗号化されたコンテンツ鍵をデータ処理装置に出力し、暗号化されたディジタルデータを記憶用鍵データで暗号化されたコンテンツ鍵とともにデータ処理装置から入力する第２のインターフェイス手段と、データ処理装置から入力された暗号化されたディジタルデータとコンテンツ鍵を記憶するメモリ手段とを備えるデータ処理システムである。

【００１５】請求項４３の発明は、データ処理装置と記憶装置との間でディジタルデータを入出力するデータ処理方法において、コンテンツ鍵をセッション鍵で暗号化するステップと、セッション鍵で暗号化されたコンテンツ鍵をデータ処理装置から記憶装置に送出するステップと、データ処理装置からのコンテンツ鍵をセッション鍵で復号するステップと、復号されたコンテンツ鍵を記憶装置の記憶用鍵データで暗号化するステップと、記憶用鍵データで暗号化されたコンテンツ鍵を記憶装置からデータ処理装置に送出するステップと、ディジタルデータを記憶装置からのコンテンツ鍵に基づいて暗号化するステップと、暗号化されたディジタルデータを記憶用鍵データで暗号化されたコンテンツ鍵とともにデータ処理装置から記憶装置に送出するステップと、データ処理装置からの暗号化されたディジタルデータとコンテンツ鍵を記憶するステップとを備えるデータ処理方法である。

【００１６】

【発明の実施の形態】以下、この発明の実施形態に係わるオーディオシステムについて説明する。図１は、一実施形態のオーディオシステム１のシステム構成図、図２は図１に示す携帯用記憶装置３および携帯用プレーヤ４の内部構成図である。図１に示すように、オーディオシステム１は、例えば、コンピュータ２、携帯用記憶装置３、携帯用プレーヤ４、ＣＤ－ＲＯＭドライブ６およびＣＤプレーヤ７を有する。

【００１７】コンピュータ２

コンピュータ２は、ネットワーク５に接続されており、例えば、EMD(Electronic Music Distribution: 電子音楽配信）などのサービスを提供する図示しないサービスプロバイダのホストコンピュータから、ネットワーク５を介してオーディオデータ（トラックデータ）を受信し、当該受信したオーディオデータを必要に応じて復号して、携帯用プレーヤ４に出力する。また、コンピュータ２は、コンテンツデータを受信するに当たって、必要に応じて、サービスプロバイダのホストコンピュータとの間で認証処理および課金処理などを行う。また、コンピュータ２は、例えば、ＣＤ－ＲＯＭドライブ６から入力したオーディオデータを携帯用プレーヤ４に出力する。

【００１８】携帯用記憶装置３

携帯用記憶装置３は、携帯用プレーヤ４に対して着脱自在とされ、例えば、メモリスティック(Memory Stick:商標）であり、フラッシュメモリなどの書き換え可能な半導体メモリを内蔵している。本明細書において、メモリカードの用語が使用されることもあるが、メモリカードは、携帯用記憶装置を指すものとして使用している。図２に示すように、携帯用記憶装置３は、例えば、主制御モジュール３１、通信インターフェイス３２、制御モジュール３３、フラッシュメモリ３４およびフラッシュメモリ管理モジュール３５を有する。

【００１９】（制御モジュール３３）図２に示すように、制御モジュール３３は、例えば、乱数発生ユニット５０、記憶ユニット５１、鍵生成／演算ユニット５２、相互認証ユニット５３、暗号化／復号ユニット５４および制御ユニット５５を有する。制御モジュール３３は、シングルチップの暗号処理専用の集積回路であり、多層構造を有し、内部のメモリセルはアルミニウム層などのダミー層に挟まれている。また、制御モジュール３３は、動作電圧または動作周波数の幅が狭く、外部から不正にデータを読み出せないように耐タンパー性を有している。乱数発生ユニット５０は、乱数発生指示を受けると、６４ビット（８バイト）の乱数を発生する。

【００２０】記憶ユニット５１は、例えば、ＥＥＰＲＯＭ(Electrically Erasable Programmable Read Only Me

mory）などの不揮発性メモリであり、認証処理に必要な鍵データなどの種々のデータを記憶している。図３は、記憶ユニット５１に記憶されているデータを説明するための図である。図３に示すように、記憶ユニット５１は、認証鍵データIK_0～IK_{31}、装置識別データID_mおよび記憶用鍵データSK_mを記憶している。

【００２１】認証鍵データIK_0～IK_{31}は、携帯用記憶装置３が携帯用プレーヤ４との間で相互認証を行う際に用いられる鍵データであり、後述するように相互認証を行う度に認証鍵データIK_0～IK_{31}のうち一の認証鍵データがランダムに選択される。なお、認証鍵データIK_0～IK_{31}および記憶用鍵データSK_mは、携帯用記憶装置３の外部から読めないようになっている。装置識別データID_mは、携帯用記憶装置３に対してユニークに付けられた識別データであり、後述するように、携帯用記憶装置３が携帯用プレーヤ４との間で相互認証を行う際に読み出されて携帯用プレーヤ４に出力される。記憶用鍵データSK_mは、後述するように、コンテンツ鍵データＣＫを暗号化してフラッシュメモリ３４に記憶する際に用いられる。

【００２２】鍵生成／演算ユニット５２は、例えば、ＩＳＯ／ＩＥＣ９７９７のＭＡＣ（Message Authentication Code）演算などの種々の演算を行って鍵データを生成する。このとき、ＭＡＣ演算には、例えば、"Block cipher Algorithm"としてＦＩＰＳＰＵＢ４６－２に規定されるＤＥＳ（Data Encryption Standard）が用いられる。ＭＡＣ演算は、任意の長さのデータを固定の長さに圧縮する一方向性ハッシュ関数演算であり、関数値が秘密鍵に依存して定まる。

【００２３】相互認証ユニット５３は、携帯用プレーヤ４からオーディオデータを入力してフラッシュメモリ３４に書き込む動作を行うのに先立って、携帯用プレーヤ４との間で相互認証処理を行う。また、相互認証ユニット５３は、フラッシュメモリ３４からオーディオデータを読み出して携帯用プレーヤ４に出力する動作を行うのに先立って、携帯用プレーヤ４との間で相互認証処理を行う。また、相互認証ユニット５３は、相互認証処理において、前述したＭＡＣ演算を行う。当該相互認証処理では、記憶ユニット５１に記憶されているデータが用いられる。

【００２４】暗号化／復号ユニット５４は、ＤＥＳ、ＩＤＥＡ、ＭＩＳＴＹなどのブロック暗号アルゴリズムでの暗号化を行う。使用するモードは、ＦＩＰＳ ＰＵＢ ８１"ＤＥＳ ＭＯＤＥＳ ＯＦ ＯＰＥＲＡＴＩＯＮ"に規定されているようなＥＣＢ（Electronic Code Book）モードおよびＣＢＣ（Cipher Block Chaining）モードである。また、暗号化／復号ユニット５４は、ＤＥＳ、ＩＤＥＡ、ＭＩＳＴＹなどのブロック復号アルゴリズムでの復号を行う。使用するモードは、上記ＥＣＢモードおよびＣＢＣモードのブロック暗号化／復号では、指定された鍵データを用いて指定されたデータを暗号化／復号する。制御ユニット５５は、乱数発生ユニット５０、記憶ユニット５１、鍵生成／演算ユニット５２、相互認証ユニット５３および暗号化／復号ユニット５４の処理を統括して制御する。

【００２５】【フラッシュメモリ３４】フラッシュメモリ３４は、例えば、３２Ｍバイトの記憶容量を有する。フラッシュメモリ３４には、相互認証ユニット５３による相互認証処理によって正当な相手であると認められたときに、携帯用プレーヤ４から入力したオーディオデータが書き込まれる。また、フラッシュメモリ３４からは、相互認証ユニット５３による相互認証処理によって正当な相手であると認められたときに、オーディオデータが読み出されて携帯用プレーヤ４に出力される。

【００２６】以下、フラッシュメモリ３４に記憶されるデータおよびそのフォーマットについて説明する。図４は、フラッシュメモリ３４に記憶されるデータを説明するための図である。図４に示すように、フラッシュメモリ３４には、例えば、再生管理ファイル１００、トラックデータファイル101_0，101_1，101_2，101_3が記憶されている。ここで、再生管理ファイル１００は101_3までのトラックデータファイル101_0～101_3の再生を管理する管理データを有し、トラックデータファイル101_0～101_3はそれぞれ対応するトラックデータ（オーディオデータ）を有している。なお、本実施形態では、トラックデータは、例えば、１曲分のオーディオデータを意味する。

【００２７】図５は、再生管理ファイルの構成を示し、図６が一つ（１曲）のＡＴＲＡＣ３データファイルの構成を示す。再生管理ファイルは、１６ＫＢ固定長のファイルである。ＡＴＲＡＣ３データファイルは、曲単位でもって、先頭の属性ヘッダと、それに続く実際の暗号化された音楽データとからなる。属性ヘッダも１６ＫＢ固定長とされ、再生管理ファイルと類似した構成を有する。

【００２８】再生管理ファイルは、ヘッダ、１バイトコードのメモリカードの名前ＮＭ１－Ｓ、２バイトコードのメモリカードの名前ＮＭ２－Ｓ、曲順の再生テーブルＴＲＫＴＢＬ、メモリカード全体の付加情報ＩＮＦ－Ｓとからなる。データファイルの先頭の属性ヘッダは、ヘッダ、１バイトコードの曲名ＮＭ１、２バイトコードの曲名ＮＭ２、トラックのキー情報等のトラック情報ＴＲＫＩＮＦ、パーツ情報ＰＲＴＩＮＦと、トラックの付加情報ＩＮＦとからなる。ヘッダには、総パーツ数、名前の属性、付加情報のサイズの情報等が含まれる。

【００２９】属性ヘッダに対してＡＴＲＡＣ３の音楽データが続く。音楽データは、１６ＫＢのブロック毎に区切られ、各ブロックの先頭にヘッダが付加されている。ヘッダには、暗号を復号するための初期値が含まれる。

なお、暗号化の処理を受けるのは、ＡＴＲＡＣ３データファイル中の音楽データのみであって、それ以外の再生管理ファイル、ヘッダ等のデータは、暗号化されない。

【００３０】図７は、再生管理ファイルＰＢＬＩＳＴのより詳細なデータ構成を示し、図８Ａ、図８Ｂは、再生管理ファイルＰＢＬＩＳＴを構成するヘッダとそれ以外の部分をそれぞれ示す。再生管理ファイルＰＢＬＩＳＴは、１クラスタ（１ブロック＝１６ＫＢ）のサイズである。ヘッダ（図８Ａ）が３２バイトである。ヘッダ以外の部分（図８Ｂ）がメモリカード全体に対する名前ＮＭ１－Ｓ（２５６バイト）、名前ＮＭ２－Ｓ（５１２バイト）、ＣＯＮＴＥＮＴＳ　ＫＥＹ、ＭＡＣ、Ｓ－ＹＭＤｈｍｓと、再生順番を管理するテーブルＴＲＫＴＢＬ（８００バイト）と、メモリカード全体に対する付加情報ＩＮＦ－Ｓ（１４７２０バイト）であり、最後にヘッダ中の情報の一部が再度記録される。これらの異なる種類のデータ群のそれぞれの先頭は、再生管理ファイル内で所定の位置となるように規定されている。

【００３１】再生管理ファイルは、（０ｘ０００００）および（０ｘ００１０）で表される先頭から３２バイト（図８Ａ）がヘッダである。なお、ファイル中で先頭から１６バイト単位で区切られた単位をスロットと称する。ファイルの第１および第２のスロットに配されるヘッダには、下記の意味、機能、値を持つデータが先頭から順に配される。なお、Ｒｅｓｅｒｖｅｄと表記されているデータは、未定義のデータを表している。通常ヌル（０ｘ００）が書かれるが、何が書かれていてもＲｅｓｅｒｖｅｄのデータが無視される。将来のバージョンでは、変更がありうる。また、この部分への書き込みは禁止する。Ｏｐｔｉｏｎと書かれた部分も使用しない場合は、全てＲｅｓｅｒｖｅｄと同じ扱いとされる。

【００３２】ＢＬＫＩＤ－ＴＬ０（４バイト）
意味：BLOCKID FILE ID
機能：再生管理ファイルの先頭であることを識別するための値
値：固定値=”ＴＬ＝０”（例えば０ｘ５４４Ｃ２Ｄ３０）

ＭＣｏｄｅ（２バイト）
意味：MAKER CODE
機能：記録した機器の、メーカー、モデルを識別するコード
値：上位１０ビット（メーカーコード）　下位６ビット（機種コード）

ＲＥＶＩＳＩＯＮ（４バイト）
意味：ＰＢＬＩＳＴの書き換え回数
機能：再生管理ファイルを書き換える度にインクリメント
値：０より始まり＋１づつ増加する

Ｓ－ＹＭＤｈｍｓ（４バイト）（Ｏｐｔｉｏｎ）
意味：信頼できる時計を持つ機器で記録した年・月・日・時・分・秒
機能：最終記録日時を識別するための値
値：２５～３１ビット　年　０～９９（１９８０～２０７９）
２１～２４ビット　月　０～１２
１６～２０ビット　日　０～３１
１１～１５ビット　時　０～２３
０５～１０ビット　分　０～５９
００～０４ビット　秒　０～２９（２秒単位）。

【００３３】ＳＮＩＣ＋Ｌ（２バイト）
意味：ＮＭ１－Ｓ領域に書かれるメモリカードの名前（１バイト）の属性を表す
機能：使用する文字コードと言語コードを各１バイトで表す
値：文字コード（Ｃ）は上位１バイトで下記のように文字を区別する
00: 文字コードは設定しない。単なる２進数として扱うこと
01: ASCII　02:ASCII+KANA　03:modified8859-1
81:MS-JIS　82:KS C 5601-1989　83:GB2312-80　90:S-JIS(for Voice)。

【００３４】言語コード（Ｌ）は下位１バイトで下記のようにEBU Tech 3258 規定に準じて言語を区別する
00: 設定しない　08:German　09:English　0A:Spanish
0F:French　15:Italian　1D:Dutch
65:Korean　69:Japanese　75:Chinese
データが無い場合オールゼロとすること。

【００３５】ＳＮ２Ｃ＋Ｌ（２バイト）
意味：ＮＭ２－Ｓ領域に書かれるメモリカードの名前（２バイト）の属性を表す
機能：使用する文字コードと言語コードを各１バイトで表す
値：上述したＳＮＩＣ＋Ｌと同一

ＳＩＮＦＳＩＺＥ（２バイト）
意味：ＩＮＦ－Ｓ領域に書かれるメモリカード全体に関する付加情報の全てを合計したサイズを表す
機能：データサイズを１６バイト単位の大きさで記述、無い場合は必ずオールゼロとすること
値：サイズは０ｘ０００１から０ｘ３９Ｃ（９２４）

Ｔ－ＴＲＫ（２バイト）
意味：TOTAL TRACK NUMBER
機能：総トラック数
値：１から０ｘ０１９０（最大４００トラック）、データが無い場合はオールゼロとすること

ＶｅｒＮｏ（２バイト）
意味：フォーマットのバージョン番号
機能：上位がメジャーバージョン番号、下位がマイナーバージョン番号

値：例　０ｘ０１００（Ｖｅｒ１．０）
　　０ｘ０２０３（Ｖｅｒ２．３）。

【００３６】上述したヘッダに続く領域に書かれるデータ（図８Ｂ）について以下に説明する。

【００３７】ＮＭ１－Ｓ
意味：メモリカード全体に関する１バイトの名前
機能：１バイトの文字コードで表した可変長の名前データ（最大で２５６）
名前データの終了は、必ず終端コード（０ｘ００）を書き込むこと
サイズはこの終端コードから計算すること、データの無い場合は少なくとも先頭（０ｘ００２０）からヌル（０ｘ００）を１バイト以上記録すること
値：各種文字コード
ＮＭ２－Ｓ
意味：メモリカード全体に関する２バイトの名前
機能：２バイトの文字コードで表した可変長の名前データ（最大で５１２）
名前データの終了は、必ず終端コード（０ｘ００）を書き込むこと
サイズはこの終端コードから計算すること、データの無い場合は少なくとも先頭（０ｘ０１２０）からヌル（０ｘ００）を２バイト以上記録すること
値：各種文字コード。

【００３８】ＣＯＮＴＥＮＴＳ　ＫＥＹ
意味：曲ごとに用意された値でＭＧ（Ｍ）で保護されてから保存される。ここでは、１曲目に付けられるＣＯＮＴＥＮＴＳ　ＫＥＹと同じ値
機能：Ｓ－ＹＭＤｈｍｓのＭＡＣの計算に必要となる鍵となる
値：０から０ｘＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦまでＭＡＣ
意味：著作権情報改ざんチェック値
機能：Ｓ－ＹＭＤｈｍｓの内容とＣＯＮＴＥＮＴＳ　ＫＥＹから作成される値
値：０から０ｘＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦまで。

【００３９】ＴＲＫ－ｎｎｎ
意味：再生するＡＴＲＡＣ３データファイルのＳＱＮ（シーケンス）番号
機能：ＴＲＫＩＮＦの中のＦＮｏを記述する
値：１から４００（０ｘ１９０）
トラックが存在しない時はオールゼロとすること
ＩＮＦ－Ｓ
意味：メモリカード全体に関する付加情報データ（例えば写真、歌詞、解説等の情報）
機能：ヘッダを伴った可変長の付加情報データ
複数の異なる付加情報が並べられることがある。それぞれにＩＤとデータサイズが付けられている。個々のヘッダを含む付加情報データは最小１６バイト以上で４バイトの整数倍の単位で構成される。その詳細については、後述する
値：付加情報データ構成を参照
Ｓ－ＹＭＤｈｍｓ（４バイト）（Ｏｐｔｉｏｎ）
意味：信頼できる時計を持つ機器で記録した年・月・日・時・分・秒
機能：最終記録日時を識別するための値、ＥＭＤの時は必須
値：２５～３１ビット　年　０～９９（１９８０～２０７９）
２１～２４ビット　月　０～１２
１６～２０ビット　日　０～３１
１１～１５ビット　時　０～２３
０５～１０ビット　分　０～５９
００～０４ビット　秒　０～２９（２秒単位）。

【００４０】再生管理ファイルの最後のスロットとして、ヘッダ内のものと同一のＢＬＫＩＤ－ＴＬ０と、ＭＣｏｄｅと、ＲＥＶＩＳＩＯＮとが書かれる。

【００４１】民生用オーディオ機器として、メモリカードが記録中に抜かれたり、電源が切れることがあり、復活した時にこれらの異常の発生を検出することが必要とされる。上述したように、ＲＥＶＩＳＩＯＮをブロックの先頭と末尾に書き込み、この値を書き換える度に＋１インクリメントするようにしている。若し、ブロックの途中で異常終了が発生すると、先頭と末尾のＲＥＶＩＳＩＯＮの値が一致せず、異常終了を検出することができる。ＲＥＶＩＳＩＯＮが２個存在するので、高い確率で異常終了を検出することができる。異常終了の検出時には、エラーメッセージの表示等の警告が発生する。

【００４２】また、１ブロック（１６ＫＢ）の先頭部分に固定値ＢＬＫＩＤ－ＴＬ０を挿入しているので、ＦＡＴが壊れた場合の修復の目安に固定値を使用できる。すなわち、各ブロックの先頭の固定値を見れば、ファイルの種類を判別することが可能である。しかも、この固定値ＢＬＫＩＤ－ＴＬ０は、ブロックのヘッダおよびブロックの終端部分に二重に記述するので、その信頼性のチェックを行うことができる。なお、再生管理ファイルＰＢＬＩＳＴの同一のものを二重に記録しても良い。

【００４３】ＡＴＲＡＣ３データファイルは、トラック情報管理ファイルと比較して、相当大きなデータ量（例えば数千のブロックが繋がる場合もある）であり、ＡＴＲＡＣ３データファイルに関しては、後述するように、ブロック番号ＢＬＯＣＫ　ＳＥＲＩＡＬが付けられている。但し、ＡＴＲＡＣ３データファイルは、通常複数のファイルがメモリカード上に存在するので、ＣＯＮＮＵＭ０でコンテンツの区別を付けた上で、ＢＬＯＣＫ　ＳＥＲＩＡＬを付けないと、重複が発生し、ＦＡＴが壊れた場合のファイルの復旧が困難となる。

【００４４】同様に、ＦＡＴの破壊までにはいたらないが、論理を間違ってファイルとして不都合のあるような

場合に、書き込んだメーカーの機種が特定できるように、メーカーコード（ＭＣｏｄｅ）がブロックの先頭と末尾に記録されている。

【００４５】図８Ｃは、付加情報データの構成を示す。付加情報の先頭に下記のヘッダが書かれる。ヘッダ以降に可変長のデータが書かれる。

【００４６】ＩＮＦ
意味：FIELD ID
機能：付加情報データの先頭を示す固定値
値：０ｘ６９
ＩＤ
意味：付加情報キーコード
機能：付加情報の分類を示す
値：０から０ｘＦＦ
ＳＩＺＥ
意味：個別の付加情報の大きさ
機能：データサイズは自由であるが、必ず４バイトの整数倍でなければならない。また、最小１６バイト以上のこと。データの終わりより余りがでる場合はヌル（０ｘ００）で埋めておくこと
値：１６から１４７８４（０ｘ３９Ｃ０）
ＭＣｏｄｅ
意味：MAKER CODE
機能：記録した機器の、メーカー、モデルを識別するコード
値：上位１０ビット（メーカーコード）　下位６ビット（機種コード）
Ｃ＋Ｌ
意味：先頭から１２バイト目からのデータ領域に書かれる文字の属性を表す
機能：使用する文字コードと言語コードを各１バイトで表す
値：前述のＳＮ１Ｃ＋Ｌと同じ
ＤＡＴＡ
意味：個別の付加情報データ
機能：可変長データです。実データの先頭は常に１２バイト目より始まり、長さ（サイズ）は最小４バイト以上、常に４バイトの整数倍でなければならない。データの最後から余りがある場合はヌル（０ｘ００）で埋めること
値：内容により個別に定義される。

【００４７】以下、トラックデータファイル101_0～101_3について説明する。図９は、トラックデータファイル101_0の構成を説明するための図である。図９に示すように、トラックデータファイル101_0は、１個のパーツからなり、当該パーツが５個のクラスタＣＬ（０），ＣＬ（１），ＣＬ（２），ＣＬ（３），ＣＬ（４）で構成されている。当該パーツは、クラスタＣＬ（０）の先頭から開始し、クラスタＣＬ（４）のサウンドユニットＳＵ（４）で終了している。なお、トラックデータファイル101_1～101_3は、基本的に、図９に示す構成をしているが、パーツ数、クラスタ数およびクラスタ内に含まれるサウンドユニットＳＵの数は、図９に示すものには限定されず、独立して決められている。

【００４８】１トラックは、１曲を意味する。１曲は、１つのＡＴＲＡＣ３データファイル（図６参照）で構成される。ＡＴＲＡＣ３データファイルは、ＡＴＲＡＣ３により圧縮されたオーディオデータである。メモリカード４０に対しては、クラスタと呼ばれる単位で記録される。１クラスタは、例えば１６ＫＢの容量である。１クラスタに複数のファイルが混じることがない。フラッシュメモリ４２を消去する時の最小単位が１ブロックである。音楽データを記録するのに使用するメモリカード４０の場合、ブロックとクラスタは、同意語であり、且つ１クラスタ＝１セクタと定義されている。

【００４９】１曲は、基本的に１パーツで構成されるが、編集が行われると、複数のパーツから１曲が構成されることがある。パーツは、録音開始からその停止までの連続した時間内で記録されたデータの単位を意味し、通常は、１トラックが１パーツで構成される。曲内のパーツのつながりは、各曲の属性ヘッダ内のパーツ情報ＰＲＴＩＮＦで管理する。すなわち、パーツサイズは、ＰＲＴＩＮＦの中のパーツサイズＰＲＴＳＩＺＥという４バイトのデータで表す。パーツサイズＰＲＴＳＩＺＥの先頭の２バイトがパーツが持つクラスタの総数を示し、続く各１バイトが先頭および末尾のクラスタ内の開始サウンドユニット（ＳＵと略記する）の位置、終了ＳＵの位置を示す。このようなパーツの記述方法を持つことによって、音楽データを編集する際に通常、必要とされる大量の音楽データの移動をなくすことが可能となる。ブロック単位の編集に限定すれば、同様に音楽データの移動を回避できるが、ブロック単位は、ＳＵ単位に比して編集単位が大きすぎる。

【００５０】ＳＵは、パーツの最小単位であり、且つＡＴＲＡＣ３でオーディオデータを圧縮する時の最小のデータ単位である。４４．１ｋＨｚのサンプリング周波数で得られた１０２４サンプル分（１０２４×１６ビット×２チャンネル）のオーディオデータを約１／１０に圧縮した数百バイトのデータがＳＵである。１ＳＵは、時間に換算して約２３ｍ秒になる。通常は、数千に及ぶＳＵによって１つのパーツが構成される。１クラスタが４２個のＳＵで構成される場合、１クラスタで約１秒の音を表すことができる。１つのトラックを構成するパーツの数は、付加情報サイズに影響される。パーツ数は、１ブロックの中からヘッダや曲名、付加情報データ等を除いた数で決まるために、付加情報が全く無い状態が最大数（６４５個）のパーツを使用できる条件となる。

【００５１】図１０は、１ＳＵがＮバイト（例えばＮ＝３８４バイト）の場合のＡＴＲＡＣ３データファイルＡ

3Dnnnnのデータ配列を示す。図１０には、データファイルの属性ヘッダ（1ブロック）と、音楽データファイル（１ブロック）とが示されている。図１０では、この2ブロック（１６×２＝３２Kバイト）の各スロットの先頭のバイト（０ｘ０００００～０ｘ７ＦＦ０）が示されている。図１１に分離して示すように、属性ヘッダの先頭から３２バイトがヘッダであり、２５６バイトが曲名領域NM１（２５６バイト）であり、５１２バイトが曲名領域NM２（５１２バイト）である。属性ヘッダのヘッダには、下記のデータが書かれる。

【００５２】ＢＬＫＩＤ－ＨＤ０（４バイト）
意味：BLOCKID FILE ID
機能：ＡＴＲＡＣ３データファイルの先頭であることを識別するための値
値：固定値＝”ＨＤ＝０”（例えば０ｘ４８４４２Ｄ３０）
ＭＣｏｄｅ（２バイト）
意味：MAKER CODE
機能：記録した機器の、メーカー、モデルを識別するコード
値：上位１０ビット（メーカーコード）　下位６ビット（機種コード）
ＢＬＯＣＫ　ＳＥＲＩＡＬ（４バイト）
意味：トラック毎に付けられた連続番号
機能：ブロックの先頭は０から始まり次のブロックは＋１づつインクリメント編集されても値を変化させない
値：０より始まり０ｘＦＦＦＦＦＦＦＦまで。
【００５３】Ｎ１Ｃ＋Ｌ（２バイト）
意味：トラック（曲名）データ（ＮＭ１）の属性を表す
機能：ＮＭ１に使用される文字コードと言語コードを各１バイトで表す
値：ＳＮ１Ｃ＋Ｌと同一
Ｎ２Ｃ＋Ｌ（２バイト）
意味：トラック（曲名）データ（ＮＭ２）の属性を表す
機能：ＮＭ２に使用される文字コードと言語コードを各１バイトで表す
値：ＳＮ１Ｃ＋Ｌと同一
ＩＮＦＳＩＺＥ（２バイト）
意味：トラックに関する付加情報の全てを合計したサイズを表す
機能：データサイズを１６バイト単位の大きさで記述、無い場合は必ずオールゼロとすること
値：サイズは０ｘ００００からＯｘ３Ｃ６（９６６）
Ｔ－ＰＲＴ（２バイト）
意味：トータルパーツ数
機能：トラックを構成するパーツ数を表す。通常は１
値：１から０ｘ２８５（６４５dec）
Ｔ－ＳＵ（４バイト）
意味：トータルＳＵ数
機能：１トラック中の実際の総ＳＵ数を表す。曲の演奏時間に相当する
値：０ｘ０１から０ｘ００１ＦＦＦＦＦ
ＩＮＸ（２バイト）（Ｏｐｔｉｏｎ）
意味：INDEX の相対場所
機能：曲のさびの部分（特徴的な部分）の先頭を示すポインタ。曲の先頭からの位置をＳＵの個数を１／４した数で指定する。これは、通常のＳＵの４倍の長さの時間（約９３ｍ秒）に相当する
値：０から０ｘＦＦＦＦ（最大、約６０８４秒）
ＸＴ（２バイト）（Ｏｐｔｉｏｎ）
意味：INDEX の再生時間
機能：ＩＮＸ-nnnで指定された先頭から再生すべき時間のＳＵの個数を１／４した数で指定する。これは、通常のＳＵの４倍の長さの時間（約９３ｍ秒）に相当する
値：０ｘ０００Ｏ：無設定　　０ｘ０１から０ｘＦＦＥ（最大６０８４秒）
０ｘＦＦＦＦ：曲の終わりまで。
【００５４】次に曲名領域NM１およびNM２について説明する。
【００５５】NM１
意味：曲名を表す文字列
機能：１バイトの文字コードで表した可変長の曲名（最大で２５６）
名前データの終了は、必ず終端コード（０ｘ００）を書き込むこと
サイズはこの終端コードから計算すること、データの無い場合は少なくとも先頭（０ｘ００２０）からヌル（０ｘ００）を１バイト以上記録すること
値：各種文字コード
NM２
意味：曲名を表す文字列
機能：２バイトの文字コードで表した可変長の名前データ（最大で５１２）
名前データの終了は、必ず終端コード（０ｘ００）を書き込むこと
サイズはこの終端コードから計算すること、データの無い場合は少なくとも先頭（０ｘ０１２０）からヌル（０ｘ００）を２バイト以上記録すること
値：各種文字コード。
【００５６】属性ヘッダの固定位置（０ｘ３２０）から始まる、８０バイトのデータをトラック情報領域ＴＲＫＩＮＦと呼び、主としてセキュリティ関係、コピー制御関係の情報を一括して管理する。図１２にＴＲＫＩＮＦの部分を示す。ＴＲＫＩＮＦ内のデータについて、配置順序に従って以下に説明する。
【００５７】ＣＯＮＴＥＮＴＳ　ＫＥＹ（８バイト）
意味：曲毎に用意された値で、メモリカードのセキュリティブロックで保護されてから保存される
機能：曲を再生する時、まず必要となる最初の鍵となる。ＭＡＣ計算時に使用される

値：0から0xFFFFFFFFFFFFFFFFまで
MAC（8バイト）
意味：著作権情報改ざんチェック値
機能：コンテンツ累積番号を含む複数のTRKINFの内容と隠しシーケンス番号から作成される値
隠しシーケンス番号とは、メモリカードの隠し領域に記録されているシーケンス番号のことである。著作権対応でないレコーダは、隠し領域を読むことができない。また、著作権対応の専用のレコーダ、またはメモリカードを読むことを可能とするアプリケーションを搭載したパーソナルコンピュータは、隠し領域をアクセスすることができる。
【0058】A（1バイト）
意味：パーツの属性
機能：パーツ内の圧縮モード等の情報を示す
値：図13を参照して以下に説明する
ただし、N＝0，1のモノラルは、bit7が1でサブ信号を0、メイン信号（L+R）のみの特別なJointモードをモノラルとして規定する。bit2，1の情報は通常の再生機は無視しても構わない。
【0059】Aのビット0は、エンファシスのオン／オフの情報を形成し、ビット1は、再生SKIPか、通常再生かの情報を形成し、ビット2は、データ区分、例えばオーディオデータか、FAX等の他のデータかの情報を形成する。ビット3は、未定義である。ビット4、5、6を組み合わせることによって、図示のように、ATRAC3のモード情報が規定される。すなわち、Nは、この3ビットで表されるモードの値であり、モノ（N＝0，1），LP（N＝2），SP（N＝4），EX（N＝5），HQ（N＝7）の5種類のモードについて、記録時間（64MBのメモリカードの場合）、データ転送レート、1ブロック内のSU数がそれぞれ示されている。1SUのバイト数は、（モノ：136バイト、LP：192バイト、SP：304バイト、EX：384バイト、HQ：512バイト）である。さらに、ビット7によって、ATRAC3のモード（0：Dual　1：Joint）が示される。
【0060】一例として、64MBのメモリカードを使用し、SPモードの場合について説明する。64MBのメモリカードには、3968ブロックがある。SPモードでは、1SUが304バイトであるので、1ブロックに53SUが存在する。1SUは、（1024／44100）秒に相当する。従って、1ブロックは、
（1024／44100）×53×（3968－16）＝4863秒＝81分
転送レートは、
（44100／1024）×304×8＝104737 bps
となる。
【0061】LT（1バイト）
意味：再生制限フラグ（ビット7およびビット6）とセキュリティバージョン（ビット5～ビット0）
機能：このトラックに関して制限事項があることを表す
値：ビット7：　0＝制限なし　　1＝制限有り
ビット6：　0＝期限内　　1＝期限切れ
ビット5～ビット0：セキュリティバージョン0（0以外であれば再生禁止とする）
FNo（2バイト）
意味：ファイル番号
機能：最初に記録された時のトラック番号、且つこの値は、メモリカード内の隠し領域に記録されたMAC計算用の値の位置を特定する
値：1から0x190（400）
MG（D）SERIAL－nnn（16バイト）
意味：記録機器のセキュリティブロック（セキュリティIC20）のシリアル番号
機能：記録機器ごとに全て異なる固有の値
値：0から0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
CONNUM（4バイト）
意味：コンテンツ累積番号
機能：曲毎に累積されていく固有の値で記録機器のセキュリティブロックによって管理される。2の32乗、42億曲分用意されており、記録した曲の識別に使用する
値：0から0xFFFFFFFF。
【0062】YMDhms－S（4バイト）（Option）
意味：再生制限付きのトラックの再生開始日時
機能：EMDで指定する再生開始を許可する日時
値：上述した日時の表記と同じ
YMDhms－E（4バイト）（Option）
意味：再生制限付きのトラックの再生終了日時
機能：EMDで指定する再生許可を終了する日時
値：上述した日時の表記と同じ
MT（1バイト）（Option）
意味：再生許可回数の最大値
機能：EMDで指定される最大の再生回数
値：1から0xFF　未使用の時は、0x00
LTのbit7の値が0の場合はMTの値は00とすること
CT（1バイト）（Option）
意味：再生回数
機能：再生許可された回数の内で、実際に再生できる回数。再生の度にデクリメントする
値：0x00～0xFF　未使用の時は、0x00である
LTのbit7が1でCTの値が00の場合は再生を禁止すること。
【0063】CC（1バイト）
意味：COPY CONTROL
機能：コピー制御

値：図１４に示すように、ビット６および７によってコピー制御情報を表し、ビット４および５によって高速ディジタルコピーに関するコピー制御情報を表し、ビット２および３によってセキュリティブロック認証レベルを表す。ビット０および１は、未定義

ＣＣの例：（ｂｉｔ７，６）１１：無制限のコピーを許可、０１：コピー禁止、００：１回のコピーを許可（ｂｉｔ３，２）００：アナログないしディジタルインからの録音、ＭＧ認証レベルは０とする

ＣＤからのディジタル録音では（ｂｉｔ７，６）は００、（ｂｉｔ３，２）は００となる

ＣＮ（１バイト）（Ｏｐｔｉｏｎ）

意味：高速ディジタルコピーＨＳＣＭＳ(High speed Serial Copy ManagementSystem)におけるコピー許可回数

機能：コピー１回か、コピーフリーかの区別を拡張し、回数で指定する。コピー第１世代の場合にのみ有効であり、コピーごとに減算する

値：００：コピー禁止、０１から０ｘＦＥ：回数、０ｘＦＦ：回数無制限。

【００６４】上述したトラック情報領域ＴＲＫＩＮＦに続いて、０ｘ０３７０から始まる２４バイトのデータをパーツ管理用のパーツ情報領域ＰＲＴＩＮＦと呼び、１つのトラックを複数のパーツで構成する場合に、時間軸の順番にＰＲＴＩＮＦを並べていく。図１５にＰＲＴＩＮＦの部分を示す。ＰＲＴＩＮＦ内のデータについて、配置順序に従って以下に説明する。

【００６５】ＰＲＴＳＩＺＥ（４バイト）

意味：パーツサイズ

機能：パーツの大きさを表す。クラスタ：２バイト（最上位）、開始ＳＵ：１バイト（上位）、終了ＳＵ：１バイト（最下位）

値：クラスタ：１から０ｘ１Ｆ４０（８０００）、開始ＳＵ：０から０ｘＡ０（１６０）、終了ＳＵ：０から０ｘＡ０（１６０）（但し、ＳＵの数え方は、０，１，２，とＯから開始する）

ＰＲＴＫＥＹ（８バイト）

意味：パーツを暗号化するための値

機能：初期値＝０、編集時は編集の規則に従うこと

値：０から０ｘＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦ

ＣＯＮＮＵＭ０（４バイト）

意味：最初に作られたコンテンツ累積番号キー

機能：コンテンツをユニークにするためのＩＤの役割

値：コンテンツ累積番号初期値キーと同じ値とされる。

【００６６】ＡＴＲＡＣ３データファイルの属性ヘッダ中には、図１０に示すように、付加情報ＩＮＦが含まれる。この付加情報は、開始位置が固定化されていない点を除いて、再生管理ファイル中の付加情報ＩＮＦ－Ｓ（図７および図８Ｂ参照）と同一である。１つまたは複数のパーツの最後のバイト部分（４バイト単位）の次を開始位置として付加情報ＩＮＦのデータが開始する。

【００６７】ＩＮＦ

意味：トラックに関する付加情報データ

機能：ヘッダを伴った可変長の付加情報データ。複数の異なる付加情報が並べられることがある。それぞれにＩＤとデータサイズが付加されている。個々のヘッダを含む付加情報データは、最小１６バイト以上で４バイトの整数倍の単位

値：再生管理ファイル中の付加情報ＩＮＦ－Ｓと同じである。

【００６８】上述した属性ヘッダに対して、ＡＴＲＡＣ３データファイルの各ブロックのデータが続く。図１６に示すように、ブロック毎にヘッダが付加される。各ブロックのデータについて以下に説明する。

【００６９】ＢＬＫＩＤ－Ａ３Ｄ（４バイト）

意味：ＢＬＯＣＫＩＤ ＦＩＬＥ ＩＤ

機能：ＡＴＲＡＣ３データの先頭であることを識別するための値

値：固定値＝”Ａ３Ｄ”（例えば０ｘ４１３３４４２０）

ＭＣｏｄｅ（２バイト）

意味：ＭＡＫＥＲ ＣＯＤＥ

機能：記録した機器の、メーカー、モデルを識別するコード

値：上位１０ビット（メーカーコード）　下位６ビット（機種コード）

ＣＯＮＮＵＭ０（４バイト）

意味：最初に作られたコンテンツ累積番号

機能：コンテンツをユニークにするためのＩＤの役割、編集されても値は変化させない

値：コンテンツ累積番号初期値キーと同じ値とされる

ＢＬＯＣＫ　ＳＥＲＩＡＬ（４バイト）

意味：トラック毎に付けられた連続番号

機能：ブロックの先頭は０から始まり次のブロックは＋１づつインクリメント編集されても値を変化させない

値：０より始まり０ｘＦＦＦＦＦＦＦＦまで

ＢＬＯＣＫ－ＳＥＥＤ（８バイト）

意味：１ブロックを暗号化するための１つの鍵

機能：ブロックの先頭は、記録機器のセキュリティブロックで乱数を生成、続くブロックは、＋１インクリメントされた値、この値が失われると、１ブロックに相当する約１秒間、音が出せないために、ヘッダとブロック末尾に同じものが二重に書かれる。編集されても値を変化させない

値：初期は８バイトの乱数

ＩＮＩＴＩＡＬＩＺＡＴＩＯＮ　ＶＥＣＴＯＲ（８バイト）

意味：ブロック毎にＡＴＲＡＣ３データを暗号化、復号化する時に必要な初期値

機能：ブロックの先頭は０から始まり、次のブロックは最後のＳＵの最後の暗号化された８バイトの値。デバイ

ドされたブロックの途中からの場合は開始ＳＵの直前の最後の８バイトを用いる。編集されても値を変化させない
値：０から０ｘＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦ
ＳＵ－ｎｎｎ
意味：サウンドユニットのデータ
機能：１０２４サンプルから圧縮されたデータ、圧縮モードにより出力されるバイト数が異なる。編集されても値を変化させない（一例として、ＳＰモードの時では、Ｎ＝３８４バイト）
値：ＡＴＲＡＣ３のデータ値。

【００７０】図１０では、Ｎ＝３８４であるので、１ブロックに４２ＳＵが書かれる。また、１ブロックの先頭の２つのスロット（４バイト）がヘッダとされ、最後の１スロット（２バイト）にＢＬＫＩＤ－Ａ３Ｄ、ＭＣｏｄｅ、ＣＯＮＮＵＭ０、ＢＬＯＣＫ　ＳＥＲＩＡＬが二重に書かれる。従って、１ブロックの余りの領域Ｍバイトは、（１６，３８４－３８４×４２－１６×３＝２０８（バイト）となる。この中に上述したように、８バイトのＢＬＯＣＫ　ＳＥＥＤが二重に記録される。

【００７１】また、サウンドユニットＳＵ（０）～（１０１）は、図２に示す暗号化／復号ユニット６４においてＣＢＣ(Cipher Block Chainning)モードで６４ビット（８バイト）の暗号化ブロックを単位として暗号化して生成された８バイトの暗号文C_iによって構成される。本実施形態では、サウンドユニットＳＵのバイト数（例えば１６０バイト）を、暗号化の単位である暗号化ブロックのバイト数（例えば８バイト）の整数倍にしている。すなわち、１サウンドユニットＳＵは例えば２０個の暗号文C_iからなる。このとき、個々の暗号文C_iは一のサウンドユニットＳＵ内に位置し、一の暗号文C_iが複数のサウンドユニットＳＵに跨がって位置することはない。

【００７２】ここで、フラッシュメモリ３４に記憶されているオーディオデータは、後述するように例えば、ＡＴＲＡＣ３方式で圧縮されており、当該圧縮の単位がサウンドユニットＳＵである。従って、携帯用記憶装置３から携帯用プレーヤ４にオーディオデータを読み出す場合には、読み出しの最小単位は当該サウンドユニットＳＵとなる。

【００７３】このようにすることで、フラッシュメモリ３４に記憶されている暗号化されたオーディオデータにアクセスする際に、暗号化ブロックの区切りを意識する必要がなくなり、当該アクセスに伴う処理負担を軽減できる。なお、各クラスタ内に含まれるサウンドユニットＳＵの数は、１個以上１０２個以下の範囲で任意である。また、オーディオデータの圧縮方式は、ＡＴＲＡＣ３などのＡＴＲＡＣ方式以外のＣＯＤＥＣ方式でもよい。

$$IK_j = f\ (MK_j,\ ID_m)$$

【００７４】ブロックシードデータＢＳは、各ブロック毎に例えば乱数を発生して生成されたデータであり、後述するように、携帯用プレーヤ４内でブロック毎にブロック鍵データＢＫを生成する際に用いられる。当該ブロックシードデータＢＳは、エラー対策としてブロック内の２箇所に格納されている。なお、各クラスタに含まれるサウンドユニットは、暗号化された順でフラッシュメモリ３４の連続したアドレスに記憶される。また、各サウンドユニット内の暗号化ブロックは、暗号化された順にフラッシュメモリ３４の連続したアドレスに記憶される。

【００７５】〔フラッシュメモリ管理モジュール３５〕フラッシュメモリ管理モジュール３５は、フラッシュメモリ３４へのデータの書き込み、フラッシュメモリ３４からのデータの読み出しなどの制御を行う。

【００７６】携帯用プレーヤ４
図２に示すように、携帯用プレーヤ４は、例えば、主制御モジュール４１、通信インターフェイス４２、制御モジュール４３、編集モジュール４４、圧縮／伸長モジュール４５、スピーカ４６、Ｄ／Ａ変換器４７およびＡ／Ｄ変換器４８を有する。

【００７７】〔主制御モジュール４１〕主制御モジュール４１は、携帯用プレーヤ４の処理を統括的に制御する。

【００７８】〔制御モジュール４３〕図２に示すように、制御モジュール４３は、例えば、乱数発生ユニット６０、記憶ユニット６１、鍵生成／鍵演算ユニット６２、相互認証ユニット６３、暗号化／復号ユニット６４および制御ユニット６５を有する。制御モジュール４３は、制御モジュール３３と同様に、シングルチップの暗号処理専用の集積回路であり、多層構造を有し、内部のメモリセルはアルミニウム層などのダミー層に挟まれている。また、制御モジュール４３は、動作電圧または動作周波数の幅が狭く、外部から不正にデータを読み出せないように耐タンパー性を有している。乱数発生ユニット６０は、乱数発生指示を受けると、６４ビット（８バイト）の乱数を発生する。記憶ユニット６１は、認証処理に必要な種々のデータを記憶している。

【００７９】図１７は、記憶ユニット６１に記憶されているデータを説明するための図である。図１７に示すように、記憶ユニット６１は、マスター鍵データMK_0～MK_{31}および装置識別データＩＤｄを記憶している。ここで、マスター鍵データMK_0～MK_{31}と、認証鍵データIK_0～IK_{31}との間には、前述した携帯用記憶装置３の装置識別データID_mを用いて、下記式（１）に示す関係がある。なお、下記式において、ｆ（ａ，ｂ）は、例えば、引数ａ，ｂから値を導出する関数である。

【００８０】
【数１】

$$\cdots\ (1)$$

但し、iは、0≦j≦31の整数。

【0081】また、記憶ユニット61における認証鍵データIK_0～IK_{31}の記憶アドレスは、例えば5ビットで表現され、それぞれ記憶ユニット51におけるマスター鍵データMK_0～MK_{31}と同じ記憶アドレスが割り当てられている。

【0082】鍵生成／鍵演算ユニット62は、例えば、ISO／IEC9797のMAC演算方式を用いた演算などの種々の演算を行って鍵データを生成する。このとき、"Block cipher Algorithm"としてFIPS PUB 46－2に規定されるDESが用いられる。

【0083】相互認証ユニット63は、例えば、コンピュータ2から入力したオーディオデータを携帯用記憶装置3に出力する動作を行うのに先立って、携帯用記憶装置3との間で相互認証処理を行う。また、相互認証ユニット63は、携帯用記憶装置3からオーディオデータを入力する動作を行うのに先立って、携帯用記憶装置3との間で相互認証処理を行う。また、相互認証ユニット63は、相互認証処理において、前述したMAC演算を行う。当該相互認証処理では、記憶ユニット61に記憶されているデータが用いられる。なお、相互認証ユニット

$$C_i = E_k\ (P_i\ XOR\ C_{i-1})$$

i：1以上の整数

P_i：平文（64ビット）

C_i：暗号文（64ビット）

XOR：排他的論理和

E_k：56ビットの鍵データkを用いたDES方式の暗号処理

上記式（2）の演算は、図18で表現される。なお、図18において、「IV」は、ブロック暗号化初期値（64ビット）であり、図2に示す携帯用記憶装置3のフラッシュメモリ34において、図8に示すようにクラスタCL内のサウンドユニットSU（0）の直前に記憶される。

【0086】なお、コンピュータ2あるいはCDプレーヤ7から入力したオーディオデータ（平文）は、ATRAC(Adaptive TRansform Audio Coder)方式を改良したATRAC3方式で圧縮されている。なお、ATRACは、MD(Mini Disk：商標)のための符号化圧縮方式で

$$P_i = C_{i-1}\ XOR\ D_k\ (C_i)$$

i：1以上の整数

P_i：平文（64ビット）

C_i：暗号文（64ビット）

XOR：排他的論理和

D_k：56ビットの鍵データkを用いたDES方式の復号処理

上記式（3）の演算は、図19で表現される。なお、図19において、「IV」は、ブロック暗号化初期値（64ビット）であり、図2に示す携帯用記憶装置3のフラッシュメモリ34において図8に示すようにクラスタC63は、必要に応じて、例えば、コンピュータ2あるいはネットワーク5上のコンピュータとの間でオーディオデータの入出力を行う動作に先立って、コンピュータ2あるいはネットワーク5上のコンピュータとの間で相互認証処理を行う。

【0084】暗号化／復号ユニット64は、前述したように、FIPS PUB 81に規定されたECBモードおよびCBCモードを選択的に用いてブロック暗号化を行う。ここで、暗号化／復号ユニット64は、CBCモードにおいて、56ビットの鍵データkを用いて、コンピュータ2あるいはCDプレーヤ7から入力したオーディオデータ（平文）を、64ビットからなる暗号化ブロックを単位として下記式（2）に基づいて暗号化して暗号化されたオーディオデータ（暗号文）を生成する。下記式（2）から分かるように、CBCモードでは、一つ前の暗号文と次の平文との排他的論理和を暗号化するため、同一の平文が入力されても異なる暗号文が出力され、解読が困難であるという利点がある。

【0085】

【数2】

$$\cdots (2)$$

あり、例えば、288kbit／sで44．1kHzサンプルのステレオ信号が、帯域分割とMDCT(Modified Discrete Cosine Transform)とを併用して符号化されている。すなわち、先ず、帯域分割フィルタで1／4，1／4，1／2の3つの帯域に分割され、それぞれの帯域の信号がダウンサンプルされ、時間領域の信号としてMDCTで周波数領域に変換され、当該MDCTの係数が適応ビット配分を行ってスカラ量子化されている。

【0087】暗号化／復号ユニット64は、FIPS81のモードのうち、前述したECBモードおよびCBCモードの復号を選択的に行う。ここで、暗号化／復号ユニット64は、CBCモードにおいて、56ビットの鍵データkを用いて、暗号文を、64ビットからなる暗号化ブロックを単位として下記式（3）に基づいて復号して平文を生成する。

【0088】

【数3】

$$\cdots (3)$$

L内のサウンドユニットSU（0）の直前に記憶されたものが用いられる。

【0089】制御ユニット65は、乱数発生ユニット60、記憶ユニット61、鍵生成／鍵演算ユニット62、相互認証ユニット63および暗号化／復号ユニット64の処理を統括的に制御する。

【0090】〔編集モジュール44〕編集モジュール44は、例えば、図4に示すように携帯用記憶装置3のフラッシュメモリ34内に記憶されたトラックデータファイル101_0～101_3を、ユーザからの操作指示に基

づいて編集して新たなトラックデータファイルを生成する。当該編集には、１個のトラックデータファイルを分割して２個のトラックデータファイルを生成する分割編集処理と、２個のトラックデータファイルを結合して１個のトラックデータファイルを生成する結合編集処理とがある。なお、当該編集にあたって、再生管理ファイル１００およびトラックデータファイル101_0～101_3が書き換えられる。編集モジュール４４における編集処理については後に詳細に説明する。

【００９１】〔圧縮／伸長モジュール４５〕圧縮／伸長モジュール４５は、例えば、携帯用記憶装置３から入力した暗号化されたオーディオデータを復号した後に再生する際に、ＡＴＲＡＣ３方式で圧縮されているオーディオデータを伸長し、当該伸長したオーディオデータをＤ／Ａ変換器４７に出力する。また、例えば、ＣＤプレーヤ７あるいはコンピュータ２から入力したオーディオデータを、携帯用記憶装置３に記憶する際に、当該オーディオデータをＡＴＲＡＣ３方式で圧縮する。

【００９２】〔Ｄ／Ａ変換器４７〕Ｄ／Ａ変換器４７は、圧縮／伸長モジュール４５から入力したデジタル形式のオーディオデータをアナログ形式のオーディオデータに変換してスピーカ４６に出力する。

【００９３】〔スピーカ４６〕スピーカ４６は、Ｄ／Ａ変換器４７から入力したオーディオデータに応じた音響を出力する。

【００９４】〔Ａ／Ｄ変換器４８〕Ａ／Ｄ変換器４８は、例えば、ＣＤプレーヤ７から入力したアナログ形式のオーディオデータをデジタル形式に変換して圧縮／伸長モジュール４５に出力する。

【００９５】以下、図１に示すオーディオシステム１の動作について説明する。

【００９６】携帯用記憶装置３への書き込み動作

図２０は、携帯用プレーヤ４から携帯用記憶装置３への書き込み動作を説明するためのフローチャートである。

【００９７】ステップＳ１：携帯用プレーヤ４から携帯用記憶装置３に、書き込み要求信号が出力される。

【００９８】ステップＳ２：携帯用記憶装置３と携帯用プレーヤ４との間で、相互認証処理を行う際に用いる認証鍵データIK_jの選択処理が行われる。当該処理については後述する。

【００９９】ステップＳ３：携帯用記憶装置３と携帯用プレーヤ４との間で相互認証処理が行われる。当該処理については後述する。

【０１００】ステップＳ４：ステップＳ３の相互認証処

$$IK_j = f(MK_j, ID_m)$$

これにより、携帯用記憶装置３と携帯用プレーヤ４とが、上記式（４）に示す関係を持つ認証鍵データIK_0～IK_{31}およびマスター鍵データMK_0～MK_{31}を有している場合には、図２１に示す処理によって同じ認証鍵データIK_jが選択される。当該選択された認証鍵データによって携帯用記憶装置３および携帯用プレーヤ４の双方が相手を正当であると認めた場合には、ステップＳ５の処理が行われ、そうでない場合には処理が終了する。

【０１０１】ステップＳ５：携帯用記憶装置３および携帯用プレーヤ４において、セッション鍵データＳｅｋが生成される。当該処理については後述する。

【０１０２】ステップＳ６：携帯用プレーヤ４から携帯用記憶装置３に、通信インターフェイス３２，４２を介して、暗号化したオーディオデータを出力して書き込む。当該処理については後述する。

【０１０３】このように、オーディオシステム１によれば、携帯用記憶装置３と携帯用プレーヤ４との間で相互認証が行われ、双方が相手を正当であると認めた場合にのみ、携帯用プレーヤ４から携帯用記憶装置３に、暗号化されたオーディオデータが書き込まれる。そのため、著作権侵害を招くようなオーディオデータの不正な複製が容易に行われることを回避できる。

【０１０４】〔認証鍵データIK_jの選択処理（図２０に示すステップＳ２）〕図２１は、認証鍵データIK_jの選択処理を説明するための図である。図２１に示すように、図２に示す携帯用プレーヤ４の乱数発生ユニット６０によって６４ビットの乱数R_jが生成される。当該乱数R_jは、携帯用プレーヤ４から携帯用記憶装置３に出力される。そして、携帯用記憶装置３の相互認証ユニット５３によって、６４ビットの乱数R_jの下位５ビットを用いて、記憶ユニット５１に記憶されている認証鍵データIK_0～IK_{31}のうち一の認証鍵データIK_j（ｊは$0 \leqq j \leqq 31$を満たす整数）が特定される。

【０１０５】また、携帯用記憶装置３の記憶ユニット５１から読み出された装置識別データID_mが、携帯用記憶装置３から携帯用プレーヤ４に出力される。

【０１０６】そして、携帯用プレーヤ４の相互認証ユニット６３によって、乱数R_jの下位５ビットを用いて、マスター鍵データMK_0～MK_{31}のうち一のマスター鍵データMK_jが特定される。

【０１０７】そして、鍵生成／鍵演算ユニット６２において、前記特定されたマスター鍵データMK_jと、携帯用記憶装置３から入力した装置識別データID_mとを用いて、下記式（４）に基づいて、認証鍵データIK_jを生成する。下記式（４）において、ｆ（ａ，ｂ）は、例えば、引数ａ，ｂから値を導出する任意の関数である。

【０１０８】

【数４】

$$\cdots (4)$$

タIK_jは、後述する相互認証処理を行う際に、秘密鍵として用いられる。また、このとき、３２個の認証鍵データIK_jのうち選択される認証鍵データは、図２１に示す処理を行う毎に乱数R_jに応じてランダムに決定される。そのため、不正な認証が成功する確率を、一の認

証鍵データを固定して用いる場合の1／32倍にすることができ、不正な認証が行われることを高い確率で回避できる。

【0109】なお、上述した実施形態では、乱数を用いて8個の認証鍵データIK_jのうちの認証鍵データを選択する場合を例示したが、携帯用記憶装置3および携帯用プレーヤ4の外部から入力した鍵指定信号に基づいて選択する認証鍵データを決定してもよい。

【0110】〔携帯用記憶装置3と携帯用プレーヤ4との間の相互認証処理（図20に示すステップS3）〕図22は、携帯用記憶装置3と携帯用プレーヤ4との間の相互認証処理を説明するための図である。なお、当該相互認証処理を開始するときには、前述した図21に示す認証鍵データIK_jの選択処理が終了しており、携帯用プレーヤ4の相互認証ユニット53と携帯用記憶装置3の相互認証ユニット63は、選択した認証鍵データIK_j、携帯用記憶装置3の装置識別データID_mを有している。

【0111】ステップS10：携帯用記憶装置3の乱数発生ユニット50において、64ビットの乱数R_{ms}を生成し、これを携帯用プレーヤ4に出力する。

【0112】ステップS11：携帯用プレーヤ4の乱数発生ユニット60において、64ビットの乱数RdおよびSdを生成する。

【0113】ステップS12：携帯用プレーヤ4の相互認証ユニット63において、図20に示すステップS2で得た認証鍵データIK_jおよび「$Rd \| R_{ms} \| ID_m$」を用いて、下記式（5）に基づいてMAC演算を行い、MAC_Aを求める。

【0114】ここで、A‖Bは、AとBの連結（nビットのAの後ろにmビットのBを結合して（n＋m）ビットとしたもの）を示す。

【0115】

【数5】

$$MAC_A = MAC(IK_j, Rd \| R_{ms} \| ID_m) \quad \cdots (5)$$

ステップS13：携帯用プレーヤ4は、「$Rd \| Sd \| MAC_A \| j$」を携帯用記憶装置3に出力する。

【0116】ステップS14：携帯用記憶装置3の相互認証ユニット53において、図20に示すステップS2で得た認証鍵データIK_jおよび「$Rd \| R_{ms} \| ID_m$」を用いて、下記式（6）に基づいてMAC演算を行い、MAC_Bを求める。

【0117】

【数6】

$$MAC_B = MAC(IK_j, Rd \| R_{ms} \| ID_m) \quad \cdots (6)$$

ステップS15：携帯用記憶装置3の相互認証ユニット53において、ステップS14で求めたMAC_BとステップS13で入力したMAC_Aとを比較し、一致していれば、携帯用プレーヤ4が適切な認証鍵データIK_jを有していることが分かるため、携帯用記憶装置3は携帯用プレーヤ4が正当な相手であると認証する。

【0118】ステップS16：携帯用記憶装置3の相互認証ユニット53において、図20に示すステップS2で得た認証鍵データIK_jおよび「$R_{ms} \| Rd$」を用いて、下記式（7）に基づいてMAC演算を行い、MAC_Cを求める。

【0119】

【数7】

$$MAC_C = MAC(IK_j, R_{ms} \| R_d) \quad \cdots (7)$$

ステップS17：携帯用記憶装置3の乱数発生ユニット50において、64ビットの乱数S_{ms}を生成する。

【0120】ステップ18：携帯用記憶装置3から携帯用プレーヤ4に、「$S_{ms} \| MAC_C$」を出力する。

【0121】ステップS19：携帯用プレーヤ4の相互認証ユニット63において、図20に示すステップS2で得た認証鍵データIK_jおよび「$R_{ms} \| Rd$」を用いて、下記式（8）に基づいてMAC演算を行い、MAC_dを求める。

【0122】

【数8】

$$MAC_d = MAC(IK_j, R_{ms} \| R_d) \quad \cdots (8)$$

ステップS20：携帯用プレーヤ4の相互認証ユニット63において、ステップS19で求めたMAC_dとステップS18で入力したMAC_Cとを比較し、一致していれば、携帯用記憶装置3が適切な認証鍵データIK_jを有していることが分かるため、携帯用プレーヤ4は携帯用記憶装置3が正当な相手であると認証する。以上の処理によって、携帯用記憶装置3と携帯用プレーヤ4との間の相互認証が行われる。

【0123】〔セッション鍵データSekの生成処理（図20に示すステップS5）〕図23は、セッション鍵データSekの生成処理を説明するための図である。なお、当該セッション鍵データSekの生成処理を開始するときには、前述した図21に示す認証鍵データIK_jの選択処理および図22に示す相互認証処理が終了しており、携帯用記憶装置3および携帯用プレーヤ4の双方は、選択した認証鍵データIK_jおよび乱数S_d，S_{ms}を有している。

【0124】ステップS30：携帯用プレーヤ4の相互認証ユニット63は、選択した認証鍵データIK_jおよび「$S_d \| S_{ms}$」を用いて、下記式（9）に基づいてMAC演算を行い、セッション鍵データSekを生成する。

【0125】

【数9】

セッション鍵データＳｅｋ＝MAC（ＩＫj，Ｓd ‖Ｓms）　・・・（９）

ステップＳ３１：携帯用記憶装置３の相互認証ユニット５３は、選択した認証鍵データＩＫj および「Ｓd ‖Ｓms」を用いて、下記式（１０）に基づいてMAC演算を行い、セッション鍵データＳｅｋを生成する。当該セッション鍵データＳｅｋは、正当な相手同士であれば、携

セッション鍵データＳｅｋ＝MAC（ＩＫj，Ｓd ‖Ｓms）　・・・（１０）

〔携帯用記憶装置３へのオーディオデータの書き込み処理（図２０に示すステップＳ６）〕図２４は、携帯用プレーヤ４から携帯用記憶装置３へのオーディオデータの書き込み処理を説明するための図である。なお、当該書き込み処理を開始するときには、前述した図２３に示すセッション鍵データＳｅｋの生成処理は終了しており、携帯用記憶装置３および携帯用プレーヤ４は同じセッション鍵データＳｅｋを有している。

【０１２７】ステップＳ４０：携帯用プレーヤ４は、乱数発生ユニット６０にトラックデータファイル毎に乱数を発生させ、当該乱数に応じたコンテンツ鍵データＣＫを生成する。

【０１２８】ステップＳ４１：携帯用プレーヤ４は、暗号化／復号ユニット６４において、ステップＳ４０で生成したコンテンツ鍵データＣＫを、セッション鍵データＳｅｋを用いて暗号化する。

【０１２９】ステップＳ４２：携帯用プレーヤ４は、ステップＳ４１で暗号化したコンテンツ鍵データＣＫを携帯用記憶装置３に出力する。

【０１３０】ステップＳ４３：携帯用記憶装置３は、ステップＳ４２で入力した暗号化されたコンテンツ鍵データＣＫを、暗号化／復号ユニット５４において復号する。

【０１３１】ステップＳ４４：携帯用記憶装置３は、暗号化／復号ユニット５４において、ステップＳ４３で復号したコンテンツ鍵データＣＫを、記憶ユニット５１か

ＴＭＫ＝ＰＫ　ＸＯＲ　ＣＫ

ステップＳ４９：携帯用プレーヤ４は、乱数発生ユニット６０にブロック毎に乱数を発生させ、当該乱数に応じたブロックシードデータＢＳを生成する。また、携帯用プレーヤ４は、当該生成したブロックシードデータＢＳを、当該ブロック内の図１０に示す対応する位置に設定する。

【０１３７】ステップＳ５０：携帯用プレーヤ４は、例

ＢＫ＝MAC（ＴＭＫ，ＢＳ）

なお、ＭＡＣ演算の他に、例えば、ＳＨＡ－１(Secure Hash Algorithm)、ＲＩＰＥＭＤ－１６０などの一方向性ハッシュ関数(one-way hash function)の入力に秘密鍵を用いた演算を行ってブロック鍵データＢＫを生成してもよい。

【０１３９】ここで、一方向性関数ｆとは、ｘよりｙ＝ｆ（ｘ）を計算することは容易であるが、逆にｙよりｘを求めることが難しい関数をいう。一方向性ハッシュ関

帯用プレーヤ４で生成したセッション鍵データＳｅｋと同じになる。

【０１２６】

【数１０】

ら読み出した記憶用鍵データＳＫｍ を用いて暗号化する。

【０１３２】ステップＳ４５：携帯用記憶装置３は、当該暗号化されたコンテンツ鍵データＣＫを携帯用プレーヤ４に出力する。

【０１３３】ステップＳ４６：携帯用プレーヤ４は、当該暗号化されたコンテンツ鍵データＣＫを、トラックデータファイル１００ｎ内のＴＲＫＩＮＦ内に設定する。

【０１３４】ステップＳ４７：携帯用プレーヤ４は、乱数発生ユニット６０にパーツ毎に乱数を発生させ、当該乱数に応じたパーツ鍵データＰＫを生成する。また、携帯用プレーヤ４は、当該生成したパーツ鍵データＰＫを、トラックデータファイル１０１ｎの管理データＰＲＴＩＮＦ内に設定する。

【０１３５】ステップＳ４８：携帯用プレーヤ４は、例えば、パーツ毎に、鍵生成／演算ユニット６２において、下記式（１１）に示すように、ステップＳ４７で生成したパーツ鍵データＰＫとコンテンツ鍵データＣＫとの排他的論理和を演算し、当該演算結果をテンポラリ鍵データＴＭＫとする。なお、テンポラリ鍵データＴＭＫの生成は、排他的論理和を用いるものには限定されず、例えば、パーツ鍵データＰＫとコンテンツ鍵データＣＫとを加算する加算演算やその他の関数演算を用いるようにしてもよい。

【０１３６】

【数１１】

・・・（１１）

えば、鍵生成／鍵演算ユニット６２において、下記式（１２）に示すように、ステップＳ４６で生成したテンポラリ鍵データＴＭＫと、ステップＳ４７で生成したブロックシードデータＢＳとを用いてＭＡＣ演算を行い、ブロック毎にブロック鍵データＢＫを生成する。

【０１３８】

【数１２】

・・・（１２）

数については、例えば、"Handbook of Applied Cryptography, CRC Press"などに詳しく記述されている。

【０１４０】ステップＳ５１：携帯用プレーヤ４は、コンピュータ２あるいは携帯用プレーヤ４から入力したオーディオデータを、圧縮／伸長モジュール４５において、ＡＴＲＡＣ３方式で圧縮する。そして、暗号化／復号ユニット６４において、ステップＳ５０で生成したブロック鍵データＢＫを用いて、前記圧縮したオーディオ

データをＣＢＣモードで暗号化する。

【０１４１】ステップＳ５２：携帯用プレーヤ４は、ステップＳ５１で暗号化したオーディオデータに属性ヘッダを付加して、通信インターフェイス３２，４２を介して、携帯用記憶装置３に出力する。

【０１４２】ステップＳ５３：携帯用記憶装置３は、ステップＳ５２で入力した暗号化されたオーディオデータと属性ヘッダを、フラッシュメモリ３４にそのまま書き込む。以上の処理によって、携帯用プレーヤ４から携帯用プレーヤ４へのオーディオデータの書き込み処理が終了する。なお、ここでは、図４のトラックデータファイル１０１０～１０１３についてのみ述べたが、携帯用プレーヤ４は、図４の再生管理ファイルについても同様に適宜更新を行う。

【０１４３】携帯用記憶装置３からの読み出し動作
図２５は、携帯用記憶装置３から携帯用プレーヤ４への読み出し動作を説明するためのフローチャートである。

【０１４４】ステップＳ６１：携帯用プレーヤ４から携帯用記憶装置３に、読み出しを要求するトラックデータ（曲）を特定した読み出し要求信号が出力される。

【０１４５】ステップＳ２：図２１を用いて前述したように、携帯用記憶装置３と携帯用プレーヤ４との間で相互認証処理を行う際に用いる認証鍵データＩＫｊの選択処理が行われる。

【０１４６】ステップＳ３：図２２を用いて前述したように、携帯用記憶装置３と携帯用プレーヤ４との間で相互認証処理が行われる。

【０１４７】ステップＳ４：ステップＳ３の相互認証処理によって携帯用記憶装置３および携帯用プレーヤ４の双方が相手を正当であると認めた場合には、ステップＳ５の処理が行われ、そうでない場合には処理が終了する。

【０１４８】ステップＳ５：携帯用記憶装置３および携帯用プレーヤ４において、セッション鍵データＳｅｋが生成される。

【０１４９】ステップＳ６３：暗号化されたオーディオデータを、通信インターフェイス３２，４２を介して、携帯用記憶装置３から携帯用プレーヤ４に読み出す。当該処理については後述する。

【０１５０】すなわち、オーディオシステム１では、携帯用記憶装置３と携帯用プレーヤ４との間で相互認証が行われ、双方が相手を正当であると認めた場合にのみ、後述するように、携帯用プレーヤ４において、携帯用記憶装置３から携帯用プレーヤ４に出力された暗号化されたコンテンツ鍵データＣＫを適切なセッション鍵データＳｅｋで解読できる。そのため、著作権侵害を招くようなオーディオデータの不正な利用が容易に行われることを回避できる。

【０１５１】〔携帯用記憶装置３からのオーディオデータの読み出し処理（図２５に示すステップＳ６３）〕図２６は、携帯用記憶装置３から携帯用プレーヤ４へのオーディオデータの読み出し処理を説明するための図である。なお、当該読み出し処理は、前述した図２０に示す書き込み処理の後に行われるため、図４に示すトラックデータファイル１０１０～１０１３には、図１０に示すように、ＴＲＩＮＦにコンテンツ鍵データＣＫが設定され、パーツ毎にパーツ鍵データＰＫが設定され、各クラスタＣＬ内にはブロックシードデータＢＳが設定されている。また、ステップＳ５の処理が終了しているため、携帯用記憶装置３および携帯用プレーヤ４は、正当な相手同士であれば、同じセッション鍵データＳｅｋを有している。

【０１５２】ステップＳ７１：携帯用記憶装置３は、フラッシュメモリ３４に記憶されている図４に示すトラックデータファイル１０１０～１０１３のうち読み出し要求信号で特定されるトラックデータに対応するトラックデータファイルを特定し、当該特定したトラックデータファイルを構成するクラスタ内のオーディオデータを、サウンドユニットＳＵを単位として読み出して携帯用プレーヤ４に出力する。携帯用記憶装置３は、また、上記トラックデータファイルの属性ヘッダを読み出して携帯用プレーヤ４に出力する。

【０１５３】ステップＳ７２：携帯用プレーヤ４は、当該入力された属性ヘッダのうち、ＴＲＩＮＦから暗号化されたコンテンツ鍵ＣＫを抽出し、携帯用記憶装置３に出力する。

【０１５４】ステップＳ７３：携帯用記憶装置３の暗号化／復号ユニット５４は、ステップＳ７２で入力されたコンテンツ鍵データＣＫを、記憶ユニット５１に記憶されている記憶用鍵データＳＫｍ を用いて復号する。

【０１５５】ステップＳ７４：携帯用記憶装置３の暗号化／復号ユニット５４は、ステップＳ７３で復号したコンテンツ鍵データＣＫを、図２５に示すステップＳ５で得られたセッション鍵データＳｅｋを用いて暗号化する。

【０１５６】ステップＳ７５：携帯用記憶装置３は、ステップＳ７４で暗号化したコンテンツ鍵データＣＫを携帯用プレーヤ４に出力する。

【０１５７】ステップＳ７６：携帯用プレーヤ４の暗号化／復号ユニット６４は、ステップＳ７３で携帯用記憶装置３から入力したコンテンツ鍵データＣＫを、セッション鍵データＳｅｋを用いて復号する。

【０１５８】ステップＳ７７：携帯用プレーヤ４の鍵生成／演算ユニット６２は、ステップＳ７６で復号されたコンテンツ鍵データＣＫと、ステップＳ７１で入力された属性ヘッダの中のＰＲＴＩＮＦに含まれるパーツ鍵データＰＫとの排他的論理和を演算し、当該演算結果をテンポラリ鍵データＴＭＫとする。

【０１５９】

【数１３】

TMK＝PK　XOR　CK

ステップＳ７８：携帯用プレーヤ４の錬生成／鍵演算ユニット６２において、ステップＳ７６で生成したテンポラリ鍵データＴＭＫと、ステップＳ７１で入力されたトラックデータファイルのクラスタ内の図１０に示すブロックシードデータＢＳとを用いて、下記式（１４）に示

BK＝MAC（TMK，BS）

ステップＳ７９：携帯用プレーヤ４は、暗号化／復号ユニット６４において、ステップＳ７８で生成したブロック鍵データＢＫを用いて、ステップＳ７１で入力したオーディオデータを復号する。このとき、オーディオデータの復号は、各ブロック毎に、それぞれ個別に求められたブロック鍵データＢＫを用いて行われる。また、復号は、暗号化の単位である８バイトのブロックを単位として行われる。

【０１６１】ステップＳ８０：携帯用プレーヤ４は、圧縮／伸長モジュール４５において、ステップＳ７９で復号したオーディオデータをＡＴＲＡＣ３方式で伸長し、当該伸長したオーディオデータを、Ｄ／Ａ変換器４７でデジタル形式に変換した後に、スピーカ４６に出力する。このとき、圧縮／伸長モジュール４５は、ステップＳ７８で復号したオーディオデータを、サウンドユニットＳＵを単位として伸長する。以上の処理によって、携帯用記憶装置３から携帯用プレーヤ４４へのオーディオデータの読み出しおよび再生が終了する。

【０１６２】〔トラックデータファイルの分割編集処理〕前述したように、携帯用プレーヤ４の編集モジュール４４は、１個のトラックデータファイルを分割して２個のトラックデータファイルを生成する分割編集処理と、２個のトラックデータファイルを結合して１個のトラックデータファイルを生成する結合編集処理とを行う。

【０１６３】先ず、分割編集処理について説明する。図２７は、携帯用プレーヤ４の編集モジュール４４によるトラックデータファイルの分割編集処理を説明するための図である。編集モジュール４４は、例えば、図２７Ａに示す１個のトラックデータファイル（１）を、図２７Ｂに示すトラックデータファイル（１）と、図２７Ｃに示すトラックデータファイル（２）とに分割する。このとき、分割の区切りとなる最小単位はサウンドユニットＳＵであり、当該例では、図２７Ｂに示すように、トラックデータファイル（１）のクラスタＣＬ（２）のサウンドユニットＳＵ（３）とＳＵ（４）との間で分割されている。

【０１６４】当該分割により、分割後のトラックデータファイル（１）のクラスタＣＬ（２）は図２８Ａに示すようになり、新たに生成されたトラックデータファイル（２）のクラスタＣＬ（０）は図２８Ｂに示すようになる。このとき、図２８Ｂに示すように、トラックデータファイル（２）のクラスタＣＬ（０）のサウンドユニットＳＵ（０）は分割前のトラックデータファイル（１）のクラスタ（２）のサウンドユニットＳＵ（４）となり、ラックデータファイル（２）のクラスタＣＬ（０）のサウンドユニットＳＵ（１）は分割前のトラックデータファイル（１）のクラスタ（２）のサウンドユニットＳＵ（５）となる。また、図２８Ｂに示すトラックデータファイル（２）のクラスタＣＬ（０）のブロック暗号化初期値ＩＶには、図２７Ａ，Ｂに示すトラックデータファイル（１）のクラスタＣＬ（２）内のサウンドユニットＳＵ（３）の最後の８バイトが設定される。

【０１６５】本実施形態では、前述したように各クラスタ内において、最初のサウンドユニットＳＵ（０）の直前にブロック暗号化初期値ＩＶを配置したことで、分割の際に、分割位置の直前の８バイトをそのままブロック暗号化初期値ＩＶとして用いれば良く、新たなトラックデータファイルを作成する際の処理を簡単にできる。また、再生時に、サウンドユニットＳＵ（０）と共に、その直前のブロック暗号化初期値ＩＶを読み出せばよいため、再生処理も簡単になる。

【０１６６】本実施形態では、分割前のトラックデータファイル（１）のコンテンツ鍵データ、パーツ鍵データおよびブロック鍵データは、それぞれＣＫ＿１、ＰＫ＿１およびＢＫ＿１である。また、分割後のトラックデータファイル（１）のコンテンツ鍵データ、パーツ鍵データおよびブロック鍵データは、それぞれＣＫ＿１’、ＰＫ＿１’およびＢＫ＿１である。また、トラックデータファイル（２）のコンテンツ鍵データ、パーツ鍵データおよびブロック鍵データは、それぞれＣＫ＿２、ＰＫ＿２およびＢＫ＿１である。

【０１６７】図２９は、携帯用プレーヤ４の編集モジュール４４において、新たなトラックデータファイル（２）のコンテンツ鍵データおよびパーツ鍵データを生成する方法を説明するための図である。分割により生成された新たなトラックデータファイル（２）は、トラックデータファイル（１）とは別に新たなコンテンツ鍵データＣＫ＿２を有する。本実施形態では、パーツ鍵データＰＫ＿２を以下に示すように算出することで、ブロック鍵データＢＫ＿１を分割前と同じにする。

【０１６８】ステップＳ９０：編集モジュール４４は、トラックデータファイルの分割指示を入力したか否かを判断し、入力したと判断した場合にはステップＳ９１の処理を実行し、入力していないと判断した場合にはステップＳ９０の処理を繰り返す。

【数１３】

・・・（１３）

すＭＡＣ演算を行い、当該演算結果をブロック鍵データＢＫとする。ブロック鍵データＢＫは、ブロック毎に求められる。

【０１６０】

【数１４】

・・・（１４）

【０１６９】ステップＳ９１：編集モジュール４４は、乱数発生ユニット６０に乱数を発生させ、当該乱数に応じたコンテンツ鍵データＣＫ＿２を新たに生成する。

【０１７０】ステップＳ９２：携帯用記憶装置３の暗号化／復号ユニット５４において、ステップＳ９１で生成したコンテンツ鍵データＣＫ＿２を、記憶ユニット５１に記憶されている記憶用鍵データＳＫｍ を用いて暗号化する。

【０１７１】ステップＳ９３：編集モジュール４４は、当該暗号化されたコンテンツ鍵データＣＫ＿２を、当該トラックデータファイルのＴＲＫＩＮＦＩに書き込む。

【０１７２】ステップＳ９４：編集モジュール４４は、トラックデータファイル（２）のパーツ鍵データＰＫ＿２を下記式（１５）に基づいて生成する。

【０１７３】

【数１５】

$$PK\_2 = CK\_1 \ XOR \ PK\_1 \ XOR \ CK\_2 \quad \cdots (15)$$

これにより、トラックデータファイル（２）について、前記式（１１）に基づいてされるテンポラリ鍵データは、トラックデータファイル（１）のテンポラリ鍵データと同じになり、前記式（１２）に基づいて生成されるブロック鍵データも分割前のブロック鍵データＢＫ＿１と同じにできる。そのため、トラックデータファイル（２）内のサウンドユニットＳＵを新たなブロック鍵データを用いて再度暗号化する必要がない。

【０１７４】ステップＳ９５：編集モジュール４４は、ステップＳ９４で生成したパーツ鍵データＰＫ＿２を、当該トラックデータファイルＰＲＴＩＮＦにそのまま書き込む。

【０１７５】このように、オーディオシステム１では、分割して新たに生成したトラックデータファイル（２）のコンテンツ鍵データとして、新たなコンテンツ鍵データＣＫ＿２を用いた場合でも、上記式（１５）に基づいてパーツ鍵データＰＫ＿２を生成することで、テンポラリ鍵データを分割前のテンポラリ鍵データと同じにできる。その結果、ブロック鍵データも分割前のブロック鍵データＢＫ＿１と同じにでき、トラックデータファイル（２）内のサウンドユニットＳＵを新たなブロック鍵データを用いて再度暗号化する必要がない。また、同様に、分割後のトラックデータファイル（１）のパーツ鍵データＰＫ＿１’も、ブロック鍵データＢＫ＿１を変えないように、コンテンツ鍵データＣＫ＿１’に応じた決定される。その結果、分割後のトラックデータファイル（１）内のサウンドユニットＳＵを新たなブロック鍵データを用いて再度暗号化する必要もない。そのため、トラックデータファイルの分割編集に伴い演算量が大幅に増加することを回避できる。なお、ここでは、図４のトラックデータファイルについてのみ述べたが、編集モジュール４４は、図４の再生管理ファイル１００についても同様に適宜更新を行う。

【０１７６】次に、トラックデータファイルの結合編集処理について説明する。図３０は、携帯用プレーヤ４の編集モジュール４４によるトラックデータファイルの結合編集処理を説明するための図である。図３０に示すように、編集モジュール４４は、例えば、図３０Ａに示すトラックデータファイル（１）と、図３０Ｂに示すトラックデータファイル（２）とを結合して、図３０Ｃに示すトラックデータファイル（３）を生成する。

【０１７７】当該結合により、結合前のトラックデータファイル（１）からなるパーツ（１）と、結合前のトラックデータファイル（２）からなるパーツ（２）とを含む新たなトラックデータファイル（３）が生成される。また、トラックデータファイル（３）のコンテンツ鍵データとして新たなコンテンツ鍵データＣＫ＿３が生成され、パーツ（１）のパーツ鍵データＰＫ＿３＿１およびパーツ（２）のパーツ鍵データＰＫ＿３＿２が後述するようにして新たに生成される。また、当該トラックデータファイル（３）のＴＲＫＩＮＦおよびＰＲＴＩＮＦに、新たに生成された鍵データが後述するように設定される。

【０１７８】また、パーツ（１）の図６に示すＰＲＴＳＩＺＥが示す開始クラスタおよび終了クラスタとして、結合前のトラックデータファイル（１）のクラスタＣＬ（０）およびＣＬ（４）がそれぞれ設定される。また、パーツ（２）のＰＲＴＳＩＺＥが示す開始クラスタおよび終了クラスタとして、結合前のトラックデータファイル（２）のクラスタＣＬ（０）およびＣＬ（５）がそれぞれ設定される。

【０１７９】図３１は、携帯用プレーヤ４の編集モジュール４４において、新たに生成したトラックデータファイル（３）のパーツ（１）および（２）のパーツ鍵データを生成する処理を説明するための図である。なお、本実施形態では、結合の対象となるトラックデータファイル（１）がコンテンツ鍵データＣＫ＿１、パーツ鍵データＰＫ＿１およびブロック鍵データＢＫ＿１を用いており、トラックデータファイル（２）がコンテンツ鍵データＣＫ＿２、パーツ鍵データＰＫ＿２およびブロック鍵データＢＫ＿２を用いてる場合を例示して説明する。

【０１８０】ここで、トラックデータファイル（３）は新たなコンテンツ鍵データＣＫ＿３を得るが、パーツ（１）および（２）のパーツ鍵データを以下に示すように算出することで、各ブロックのブロック鍵データＢＫ＿１およびＢＫ＿２を結合前と同じにできる。

【０１８１】ステップＳ１００：編集モジュール４４は、トラックデータファイルの結合指示を入力したか否かを判断し、入力したと判断した場合にはステップＳ１０１の処理を実行し、入力していないと判断した場合に

はステップＳ１００の処理を繰り返す。

【０１８２】ステップＳ１０１：編集モジュール４４は、乱数発生ユニット６０に乱数を発生させ、当該乱数に応じたコンテンツ鍵データＣＫ＿３を新たに生成する。

【０１８３】ステップＳ１０２：携帯用記憶装置３の暗号化／復号ユニット５４において、ステップＳ１０１で生成したコンテンツ鍵データＣＫ＿３を、記憶ユニット５１に記憶されている記憶用鍵データＳＫm を用いて暗号化する。

$$PK\_3\_1 = CK\_1 \quad XOR \quad PK\_1 \quad XOR \quad CK\_3 \qquad \cdots (16)$$

これにより、前記式（１１）に基づいて生成されるパーツ（１）のテンポラリ鍵データを結合前のトラックデータファイル（１）のテンポラリ鍵データと同じにでき、その結果、前記式（１２）に基づいて生成されるパーツ（１）のブロック鍵データも結合前のトラックデータファイル（１）のブロック鍵データＢＫ＿１と同じにできる。そのため、パーツ（１）のサウンドユニットＳＵを新たなブロック鍵データを用いて再度暗号化する必要がない。

【０１８４】ステップＳ１０３：編集モジュール４４は、当該暗号化されたコンテンツ鍵データＣＫ＿３を当該トラックデータファイルのＴＲＫＩＮＦに書き込む。

【０１８５】ステップＳ１０４：編集モジュール４４は、トラックデータファイル（３）のパーツ（１）のパーツ鍵データＰＫ＿３＿１を下記式（１６）に基づいて生成する。

【０１８６】

【数１６】

$$PK\_3\_1 = CK\_1 \quad XOR \quad PK\_1 \quad XOR \quad CK\_3 \qquad \cdots (16)$$

これにより、前記式（１１）に基づいて生成されるパーツ（２）のテンポラリ鍵データを結合前のトラックデータファイル（２）のテンポラリ鍵データと同じにでき、その結果、前記式（１２）に基づいて生成されるパーツ（２）のブロック鍵データも結合前のトラックデータファイル（２）のブロック鍵データＢＫ＿２と同じにできる。そのため、パーツ（２）のサウンドユニットＳＵを新たなブロック鍵データを用いて再度暗号化する必要がない。

【０１８７】ステップＳ１０５：編集モジュール４４は、トラックデータファイル（３）のパーツ（２）のパーツ鍵データＰＫ＿３＿２を下記式（１７）に基づいて生成する。

【０１８８】

【数１７】

$$PK\_3\_2 = CK\_2 \quad XOR \quad PK\_2 \quad XOR \quad CK\_3 \qquad \cdots (17)$$

【０１８９】ステップＳ１０６：編集モジュール４４は、ステップＳ１０４で生成したパーツ鍵データＰＫ＿３＿１をトラックデータファイル（３）のパーツ（１）のＰＲＴＩＮＦにそのまま書き込む。

【０１９０】ステップＳ１０７：編集モジュール４４は、ステップＳ１０５で生成したパーツ鍵データＰＫ＿３＿２をトラックデータファイル（３）のパーツ（２）のＰＲＴＩＮＦにそのまま書き込む。

【０１９１】このように、オーディオシステム１では、結合して新たに生成したトラックデータファイル（３）のコンテンツ鍵データとして、新たなコンテンツ鍵データＣＫ＿３を用いた場合でも、上記式（１６）および（１７）に基づいてパーツ鍵データＰＫ＿３＿１およびＰＫ＿３＿２を生成することで、各パーツのテンポラリ鍵データを結合前と同じにできる。その結果、各パーツのブロック鍵データも結合前のブロック鍵データＢＫ＿１およびＢＫ＿２とそれぞれ同じにでき、パーツ（１）および（２）内のサウンドユニットＳＵを新たなブロック鍵データを用いて再度暗号化する必要がない。そのため、トラックデータファイルの結合編集に伴い演算量が大幅に増加することを回避できる。なお、ここでは、図４のトラックデータファイルについてのみ述べたが、編集モジュール４４は、図４の再生管理ファイルについても同様に適宜更新を行う。

【０１９２】この発明は、上述した実施形態等に限定されるものでは無く、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えば、上述した実施形態では、ＡＴＲＡＣ３方式の圧縮の単位であるサウンドユニットＳＵのバイト数（１６０バイト）が、ＣＢＣモードの暗号化の単位である暗号化ブロックのバイト数（８バイト）の整数倍になる場合を例示したが、この発明は、例えば、整数倍にならない場合には、サウンドユニットＳＵにデータ長調整用のデータであるパディング(padding) を挿入して調整するようにしてもよい。

【０１９３】また、上述した実施形態では、携帯用記憶装置３と携帯用プレーヤ４との間で相互認証処理を行う場合に、図２２に示すように、先ず始めに携帯用記憶装置３で生成した乱数R_{ms}を携帯用プレーヤ４に出力する場合を例示したが、先ず始めに携帯用プレーヤ４で生成した乱数を携帯用記憶装置３に出力するようにしてもよい。

【０１９４】また、上述した実施形態では、図２１に示すように、記憶ユニット５１および６１に３２組の認証鍵データおよびマスター鍵データを記憶した場合を例示したが、これらの組の数は２以上であれば任意である。

【０１９５】また、上述した実施形態では、図２１に示すように、携帯用プレーヤ４において、マスター鍵デー

タMK_0～MK_{31}から認証鍵データIK_0～IK_{31}を生成する場合を例示したが、携帯用プレーヤ４に、携帯用記憶装置３と同じように、認証鍵データIK_0～IK_{31}を記憶し、乱数R_jに応じた認証鍵データを選択するようにしてもよい。

【０１９６】また、上述した実施形態では、図２１に示すように、携帯用記憶装置３および携帯用プレーヤ４において、携帯用プレーヤ４で生成した乱数R_jを用いて、認証鍵データIK_jおよびマスター鍵データMK_jを選択する場合を例示したが、携帯用記憶装置３で生成した乱数を用いてもよいし、携帯用記憶装置３および携帯用プレーヤ４の双方で発生した乱数を用いてもよい。

【０１９７】また、上述した実施形態では、図２１に示すように、携帯用記憶装置３および携帯用プレーヤ４において乱数R_jに基づいて認証鍵データIK_jおよびマスター鍵データMK_jを選択する場合を例示したが、この発明は、例えば、携帯用記憶装置３および携帯用プレーヤ４に外部から５ビットの鍵選択指示データを入力し、当該鍵選択指示データで指示される相互に対応する認証鍵データIK_jおよびマスター鍵データMK_jを、携帯用記憶装置３および携帯用プレーヤ４で選択してもよい。

【０１９８】また、上述した実施形態では、トラックデータとしてオーディオデータを含むデータを例示したが、この発明は、その他、動画像データ、静止画像データ、文書データおよびプログラムデータなどを含むトラックデータをフラッシュメモリ３４に記憶する場合にも適用できる。

【０１９９】

【発明の効果】以上説明したように、この発明のデータ処理システムおよびその方法によれば、トラックデータを第３の鍵データを用いて暗号化し記憶装置に記憶した後に、第１の鍵データが変更された場合でも、第３の鍵データが変更されることはなく、トラックデータを復号して再度暗号化を行う必要がなくなる。そのため、第１の鍵データが変更された場合のデータ処理量を大幅に削減できる。

【図面の簡単な説明】

【図１】この発明の一実施形態のオーディオシステムのシステム構成を示すブロック図である。

【図２】携帯用記憶装置および携帯用プレーヤの内部構成を示すブロック図である。

【図３】携帯用記憶装置内の記憶ユニットに記憶されているデータを説明するための略線図である。

【図４】携帯用記憶装置のフラッシュメモリに記憶されるデータを説明するための略線図である。

【図５】再生管理ファイルのデータ構成を概略的に示す略線図である。

【図６】データファイルのデータ構成を概略的に示す略線図である。

【図７】再生管理ファイルのデータ構成をより詳細に示す略線図である。

【図８】再生管理ファイルの各部分と付加情報領域の構成を示す略線図である。

【図９】携帯用プレーヤの記憶ユニットに記憶されているデータを説明するための略線図である。

【図１０】データファイルのデータ構成をより詳細に示す略線図である。

【図１１】データファイルの属性ヘッダの一部を示す略線図である。

【図１２】データファイルの属性ヘッダの一部を示す略線図である。

【図１３】録音モードの種類と、各録音モードにおける録音時間等を示す略線図である。

【図１４】コピー制御情報を説明するための略線図である。

【図１５】データファイルの属性ヘッダの一部を示す略線図である。

【図１６】データファイルの各データブロックのヘッダを示す略線図である。

【図１７】携帯用プレーヤの記憶ユニットに記憶されているデータを説明するための略線図である。

【図１８】携帯用プレーヤの暗号化／復号ユニットのＣＢＣモードにおける暗号化処理を説明するための略線図である。

【図１９】携帯用プレーヤの暗号化／復号ユニットのＣＢＣモードにおける復号処理を説明するための略線図である。

【図２０】携帯用プレーヤから携帯用記憶装置への書き込み動作を説明するためのフローチャートである。

【図２１】相互認証ユニットによる認証鍵データIK_jの選択処理を説明するための略線図である。

【図２２】携帯用記憶装置と携帯用プレーヤとの間の相互認証処理を説明するためのフローチャートである。

【図２３】セッション鍵データＳｅｋの生成処理を説明するための略線図である。

【図２４】携帯用プレーヤから携帯用記憶装置へのオーディオデータの書き込み処理を説明するためのフローチャートである。

【図２５】携帯用記憶装置から携帯用プレーヤへの読み出し動作を説明するためのフローチャートである。

【図２６】携帯用記憶装置から携帯用プレーヤへのオーディオデータの読み出し処理を説明するためのフローチャートである。

【図２７】携帯用プレーヤの編集モジュールによるトラックデータファイルの分割編集処理を説明するための略線図である。

【図２８】分割編集処理を行った後のクラスタ内のデータを説明するための略線図である。

【図２９】携帯用プレーヤの編集モジュールにおいて、

分割編集時に、新たなトラックデータファイルのコンテンツ鍵データおよびパーツ鍵データを生成する方法を説明するためのフローチャートである。

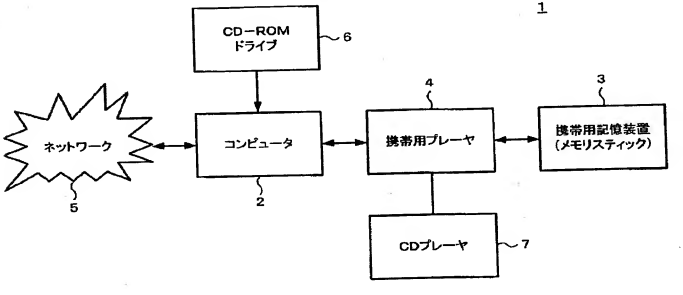
【図３０】携帯用プレーヤの編集モジュールによるトラックデータファイルの結合編集処理を説明するための略線図である。

【図３１】携帯用プレーヤ４の編集モジュールにおいて、新たに生成したトラックデータファイル（３）のパーツ（１）および（２）のパーツ鍵データを生成する処理を説明するための略線図である。

【符号の説明】

１・・・オーディオシステム、２・・・コンピュータ、３・・・携帯用記憶装置、４・・・携帯用プレーヤ、５・・・ネットワーク、３３，４３・・・制御モジュール、５０，６０・・・乱数発生ユニット、５１，６１・・・記憶ユニット、５２，６２・・・鍵生成／演算ユニット、５３，６３・・・相互認証ユニット、５４，７４・・・暗号化／復号ユニット、５５，６５・・・制御ユニット、３４・・・フラッシュメモリ、４４・・・編集モジュール、４５・・・圧縮／伸長モジュール、４６・・・スピーカ

【図１】



【図３】

携帯用記憶装置3の記憶ユニット51に記憶されるデータ

認証鍵データ　IK_0
IK_1
IK_2
IK_3
⋮
IK_{30}
IK_{31}
装置識別データ　ID_0
記憶用鍵データ　SK_m

【図５】

再生管理ファイル

Header
NM1−S
NM2−S
TRKTBL
INF−S

【図１３】

bit7:ATRAC3のモード　0:Dual　1:Joint
bit5,4　2chのMはモードの値

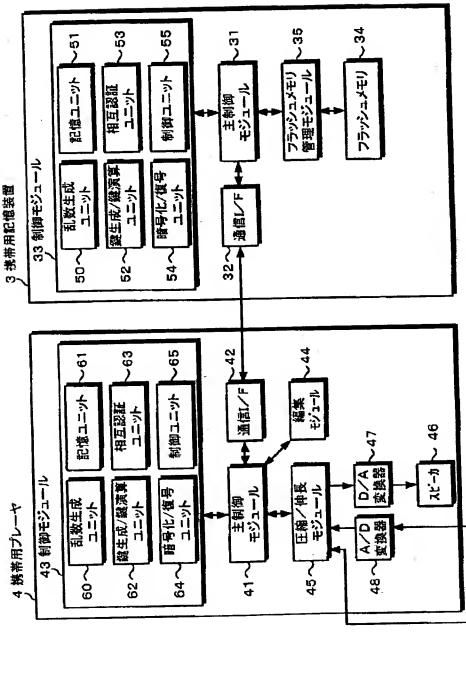
N	モード	時間	転送レート	SU	バイト
7	HQ	47min	176kbps	31SU	512
6		56min	146kbps	38SU	424
5	EX	64min	132kbps	42SU	384
4	SP	81min	105kbps	53SU	304
3		90min	94kbps	59SU	272
2	LP	128min	66kbps	84SU	192
1	mono	161min	47kbps	119SU	136
0	mono	258min	33kbps	169SU	96

bit3:Reserved
bit2:データ区分　0:オーディオ　1:その他
bit1:再生SKIP　0:通常再生　1:SKIP
bit0:エンファシス　0:OFF　1:ON(50/15μs)

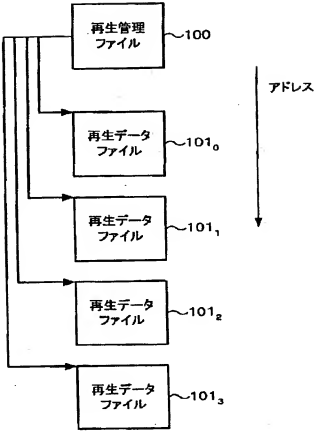
【図１１】

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID−HD0				Reserved		MDcde		Reserved				BLOCK SERIAL			
0x0010	N1C+L		N2C+L		INFSIZE		T−PRT		T−SU				INX		XT	
0x0020	NM1(256)															
0x0120	NM2(512)															
0x0310																

【図２】

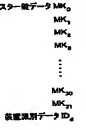

3 携帯用記憶装置
33 制御モジュール
50 乱数生成ユニット
52 鍵生成/鍵演算ユニット
54 暗号化/復号ユニット
61 記憶ユニット
63 相互認証ユニット
65 制御ユニット
32 通信I/F
31 主制御モジュール
35 フラッシュメモリ管理モジュール
34 フラッシュメモリ
4 携帯用プレーヤ
43 制御モジュール
60 乱数生成ユニット
62 鍵生成/鍵演算ユニット
64 暗号化/復号ユニット
61 記憶ユニット
63 相互認証ユニット
65 制御ユニット
42 通信I/F
41 主制御モジュール
44 伸張モジュール
45 圧縮/伸長モジュール
48 A/D変換器
47 D/A変換器
46 スピーカ
オーディオデータ
オーディオデータ
(コンピュータ2から)
(CDプレーヤ7から)

【図４】



【図１７】

携帯用プレーヤ4の記憶モジュール41に記憶されるデータ



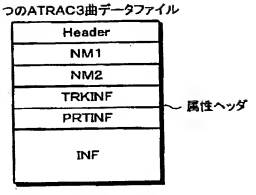
携帯用記憶装置3のフラッシュメモリ34の記憶データ

【図７】

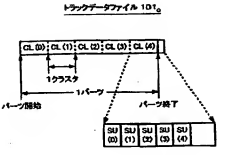
再生管理ファイル(PBLIST)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0×0000	BLKID−TL0				Reserved		MCode		REVISION				Reserved			
0×0010	SN1C−L		SN2C−L		SINFSIZE		T−TRK		VerNo		Reserved					
0×0020	NM1−S(256)															
0×0120	NM2−S(512)															
0×0320	Reserved								CONTENTSKEY							
0×0330	Reserved								MAC							
	Reserved												S−YMDhms			
0×0350	TRK−001		TRK−002		TRK−003		TRK−004		TRK−005		TRK−006		TRK−007		TRK−008	
	TRK−009		TRK−010		TRK−011		TRK−012		TRK−013		TRK−014		TRK−015		TRK−016	
0×0660	TRK−393		TRK−394		TRK−395		TRK−396		TRK−397		TRK−398		TRK−399		TRK−400	
0×0647	INF−S(14720)															
0×3FF0	BLKID−TL0				Reserved		MCode		REVISION				Reserved			

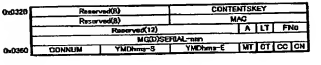
【図６】



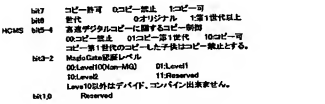
【図９】



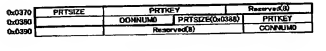
【図１２】



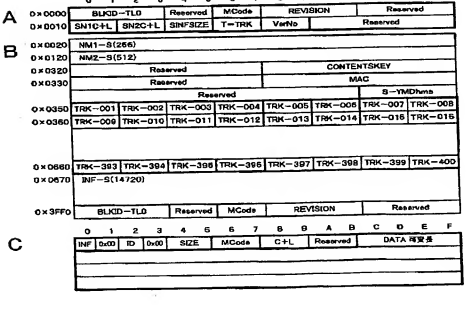
【図１４】



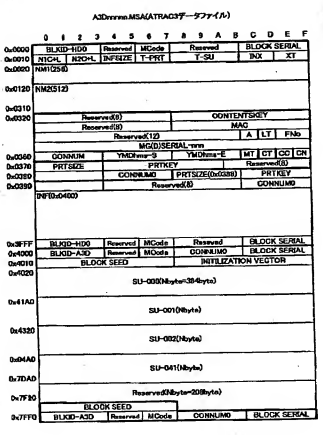
【図１５】



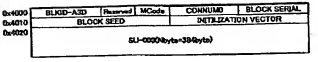
【図８】



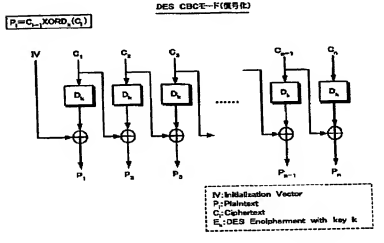
【図１０】



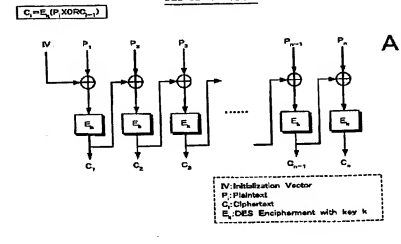
【図１６】



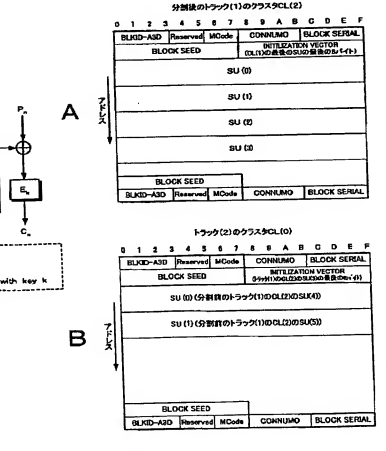
【図１９】



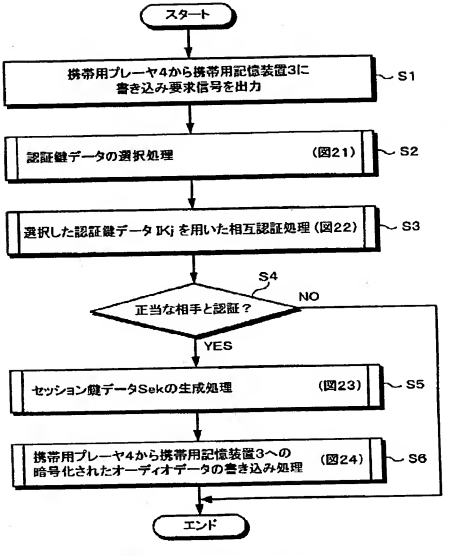
【図１８】



【図２８】

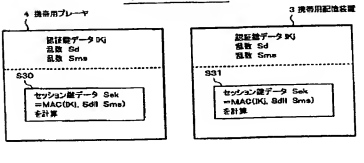


【図２０】

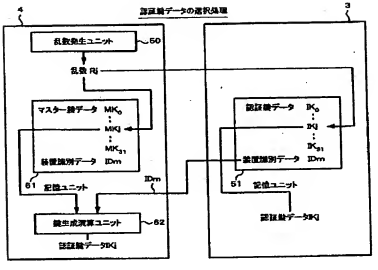


携帯用記憶装置3への書込処理

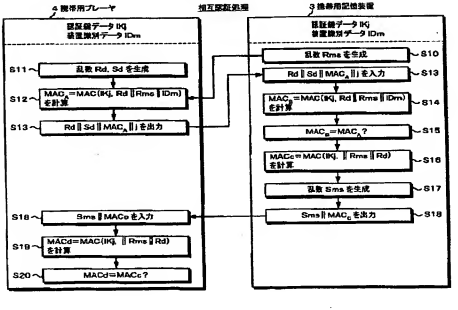
【図２３】



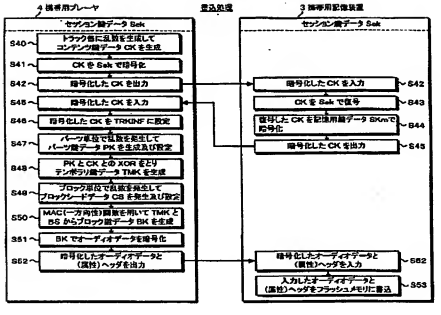
【図２１】


4
認証鍵データの選択処理
3
乱数発生ユニット
50
乱数 Rj
マスター鍵データ MK0
MKj
MK31
装置識別データ IDm
51 記憶ユニット
IDm
鍵生成演算ユニット
52
認証鍵データBKj
認証鍵データ BK0
BKj
BK31
装置識別データ IDm
51 記憶ユニット
認証鍵データBKj

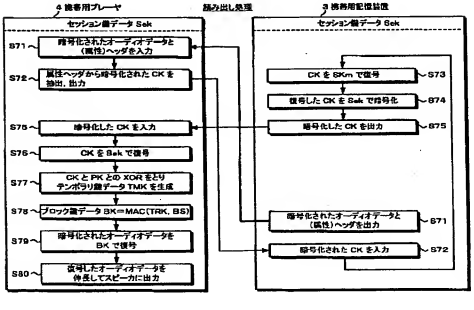
【図２２】


4 携帯用プレーヤ
認証鍵データ BKj
装置識別データ IDm
相互認証処理
3 携帯用記憶装置
認証鍵データ BKj
装置識別データ IDm
S11 乱数 Rd, Sd を生成
S12 MAC_A=MAC(BKj, Rd ‖ Rms ‖ IDm) を計算
S13 Rd ‖ Sd ‖ MAC_A ‖ j を出力
S10 乱数 Rms を生成
S13 Rd ‖ Sd ‖ MAC_A ‖ j を入力
S14 MAC_B=MAC(BKj, Rd ‖ Rms ‖ IDm) を計算
S15 MAC_B=MAC_A ?
S16 MACc=MAC(BKj, ‖ Rms ‖ Rd) を計算
S17 乱数 Sms を生成
S18 Sms ‖ MAC_C を出力
S18 Sms ‖ MACc を入力
S19 MACd=MAC(BKj, ‖ Rms ‖ Rd) を計算
S20 MACd=MACc ?

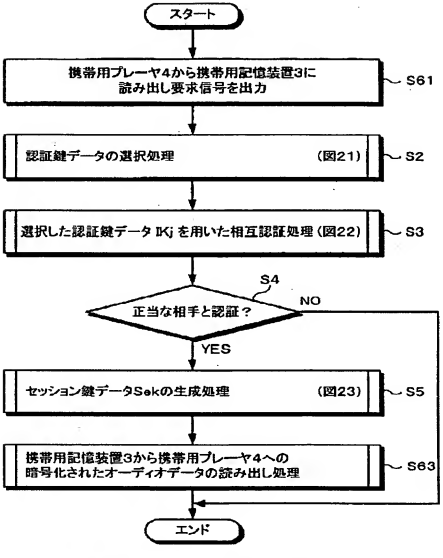
【図２４】


4 携帯用プレーヤ
書込処理
3 携帯用記憶装置
セッション鍵データ Sek
セッション鍵データ Sek
S40 ドラック毎に乱数を生成して コンテンツ鍵データ CK を生成
S41 CK を Sek で暗号化
S42 暗号化した CK を出力
暗号化した CK を入力 S42
S43 CK を Sek で復号
S44 復号した CK を記憶用鍵データ BKm で再暗号化
S45 暗号化した CK を出力
S46 暗号化した CK を入力
S47 TRKINF に設定
S47 パーツ毎独立で乱数を発生して パーツ鍵データ PK を生成及び設定
S48 PK と CK との XOR をとり テンポラリ鍵データ TMK を生成
S49 ブロック部位で乱数を発生して ブロックシードデータ CS を発生及び設定
S50 MAC(一方向性)関数を用いて TMK と BS からブロック鍵データ BK を生成
S51 BK でオーディオデータを暗号化
S52 暗号化したオーディオデータと (属性)ヘッダを出力
暗号化したオーディオデータと (属性)ヘッダを入力 S52
入力したオーディオデータと (属性)ヘッダをフラッシュメモリに書込 S53

【図２６】

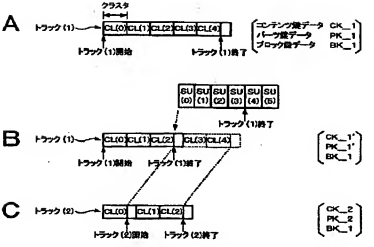

4 携帯用プレーヤ
読み出し処理
3 携帯用記憶装置
セッション鍵データ Sek
セッション鍵データ Sek
S71 暗号化されたオーディオデータと (属性)ヘッダを入力
S72 属性ヘッダから暗号化された CK を 抽出、出力
CK を BKm で復号 S73
復号した CK を Sek で暗号化 S74
S75 暗号化した CK を入力
暗号化した CK を出力 S75
S76 CK を Sek で復号
S77 CK と PK との XOR をとり テンポラリ鍵データ TMK を生成
S78 ブロック鍵データ BK=MAC(TRK, BS)
S79 暗号化されたオーディオデータを BK で復号
S80 復号したオーディオデータを 伸長してスピーカに出力
暗号化されたオーディオデータと (属性)ヘッダを出力 S71
暗号化された CK を入力 S72

【図２５】



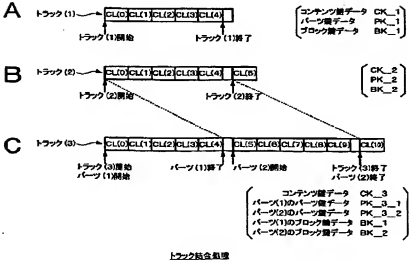
携帯用記憶装置3からの読み出し処理

【図２７】



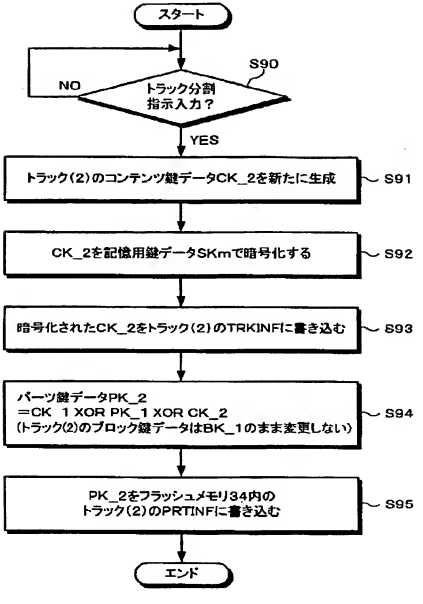
トラックの分割編集

【図３０】

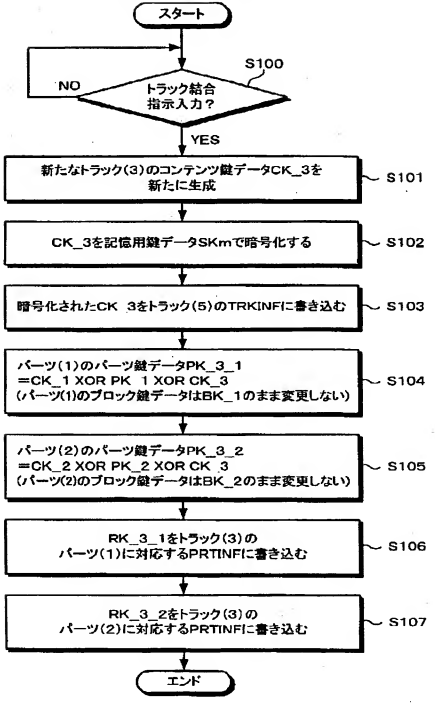


トラック統合処理

【図２９】


スタート
S90
NO
トラック分割
指示入力？
YES
トラック(2)のコンテンツ鍵データCK_2を新たに生成
S91
CK_2を記憶用鍵データSKmで暗号化する
S92
暗号化されたCK_2をトラック(2)のTRKINFに書き込む
S93
パーツ鍵データPK_2
=CK_1 XOR PK_1 XOR CK_2
(トラック(2)のブロック鍵データはBK_1のまま変更しない)
S94
PK_2をフラッシュメモリ34内の
トラック(2)のPRTINFに書き込む
S95
エンド

【図３１】



【手続補正書】
【提出日】平成１２年４月４日（２０００．４．４）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項１
【補正方法】変更
【補正内容】
【請求項１】　単数または複数の関連するモジュールから構成されるトラックデータを、当該トラックデータに割り当てられた第１の鍵データおよび上記モジュール毎に割り当てられた第２の鍵データを用いて暗号化して記憶装置に出力するデータ処理装置において、
上記モジュール毎に、上記第１の鍵データおよび上記モジュールに割り当てられた上記第２の鍵データから第３の鍵データを算出する鍵データ算出手段と、

上記トラックデータを上記モジュール毎に当該モジュールの上記第３の鍵データに応じて暗号化して上記記憶装置に出力する暗号化手段とを有し、
上記鍵データ算出手段は、上記第１の鍵データに変更があった場合に、上記第３の鍵データを変更しないように、上記モジュール毎に上記第２の鍵データを変更するデータ処理装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】請求項３
【補正方法】変更
【補正内容】
【請求項３】　請求項１において、
上記モジュールは、単数または複数のサブモジュールを有し、上記サブモジュール毎に第４の鍵データがさらに割り当てられている場合に、上記鍵データ算出手段は、上記サブモジュール毎に、上記第３の鍵データおよび上記サブモジュールに割り当てられた上記第４の鍵データから第５の鍵データを算出し、
上記暗号化手段は、上記トラックデータを上記サブモジュール毎に当該サブモジュールの上記第５の鍵データを用いて暗号化して上記記憶装置に出力するデータ処理装置。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】請求項９
【補正方法】変更
【補正内容】
【請求項９】　請求項８において、
上記データ処理装置は、
上記暗号化手段によって暗号化された上記第１の鍵データと上記第２の鍵データとを上記記憶装置に書き込むデータ処理装置。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００５
【補正方法】変更
【補正内容】
【０００５】
【課題を解決するための手段】上述した課題を解決するために、請求項１の発明は、単数または複数の関連するモジュールから構成されるトラックデータを、当該トラックデータに割り当てられた第１の鍵データおよびモジュール毎に割り当てられた第２の鍵データを用いて暗号化して記憶装置に出力するデータ処理装置において、モジュール毎に、第１の鍵データおよびモジュールに割り当てられた第２の鍵データから第３の鍵データを算出する鍵データ算出手段と、トラックデータをモジュール毎に当該モジュールの第３の鍵データに応じて暗号化して記憶装置に出力する暗号化手段とを有し、鍵データ算出手段は、第１の鍵データに変更があった場合に、第３の鍵データを変更しないように、モジュール毎に第２の鍵データを変更するデータ処理装置である。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】変更
【補正内容】
【００２７】図５は、再生管理ファイルの構成を示し、図６が一つ（１曲）のトラックデータファイル（以下においてＡＴＲＡＣ３データファイルの用語がさすものもトラックデータファイルと同義である）の構成を示す。再生管理ファイルは、１６ＫＢ固定長のファイルである。ＡＴＲＡＣ３データファイルは、曲単位でもって、先頭の属性ヘッダと、それに続く実際の暗号化された音楽データとからなる。属性ヘッダも１６ＫＢ固定長とされ、再生管理ファイルと類似した構成を有する。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００６１
【補正方法】変更
【補正内容】
【００６１】ＬＴ（１バイト）
意味：再生制限フラグ（ビット７およびビット６）とセキュリティバージョン（ビット５～ビット０）
機能：このトラックに関して制限事項があることを表す
値：ビット７：　０＝制限なし　　１＝制限有り
ビット６：　０＝期限内　　１＝期限切れ
ビット５～ビット０：セキュリティバージョン０（０以外であれば再生禁止とする）
ＦＮｏ（２バイト）
意味：ファイル番号
機能：最初に記録された時のトラック番号、且つこの値は、メモリカード内の隠し領域に記録されたＭＡＣ計算用の値の位置を特定する
値：１から０ｘ１９０（４００）
ＭＧ（Ｄ）ＳＥＲＩＡＬ－ｎｎｎ（１６バイト）
意味：記録機器のセキュリティブロック（制御モジュール４３）のシリアル番号
機能：記録機器ごとに全て異なる固有の値
値：０から0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
ＣＯＮＮＵＭ（４バイト）
意味：コンテンツ累積番号
機能：曲毎に累積されていく固有の値で記録機器のセキュリティブロックによって管理される。２の３２乗、４２億曲分用意されており、記録した曲の識別に使用する
値：０から０ｘＦＦＦＦＦＦＦＦ。

フロントページの続き

(51) Int. Cl.[7]	識別記号	FI		テーマコード(参考)
G10L 19/00		G10L 9/00	N	
G11B 27/031		H04L 9/00	601Z	
H04L 9/08			641	
9/14		G11B 27/02	A	